PCT/JP2004/010068

08. 7. 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

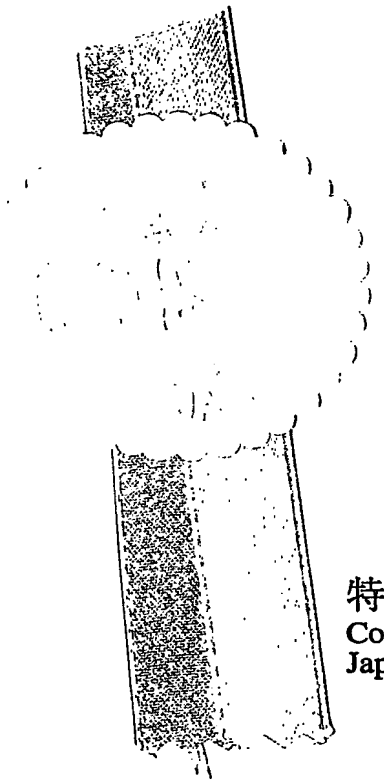
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月　８日

出願番号
Application Number: 特願２００３－２７１９２９

[ST. 10/C]: [ＪＰ２００３－２７１９２９]

出願人
Applicant(s): 松下電器産業株式会社



２００４年　８月１２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０７２０６２

【書類名】　特許願
【整理番号】　2022550237
【提出日】　平成15年 7月 8日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　館林　誠
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山本　直紀
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　石原　秀志
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、
前記再生装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、
前記読出装置は、前記記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする認証システム。
【請求項２】
前記認証システムであって、
前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、
前記再生装置は、保持する証明書のＩＤ番号が含まれる２つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする請求項１記載の認証システム。
【請求項３】
前記認証システムであって、
前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする請求項２記載の認証システム。
【請求項４】
前記認証子システムであって、
記録媒体の代わりに通信媒体を利用することを特徴とする請求項１記載の認証システム。
【請求項５】
認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、
前記再生装置は、前記読出装置が読み出した第１の認証用データを受信する受信部と、前記第１の認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第２の認証用データを受信する受信部と、前記第2の認証用データの正当性を検証する検証部と、前記検証後に前記第２の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、
前記読出装置は、前記記録媒体から読み出した第１の認証用データ、並びに第２の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする認証システム。
【請求項６】
前記認証システムであって、
前記読出装置が前記再生装置を認証する前記第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、
前記再生装置は、保持する証明書のＩＤ番号が含まれる2つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする請求項５記載の認証システム。

【請求項７】

前記認証システムであって、

前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする請求項６記載の認証システム。

【請求項８】

前記認証システムであって、

前記読出装置が前記再生装置を認証する前記第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、保持する証明書のＩＤ番号と一致するＩＤ番号を前記第１の認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする請求項５記載の認証システム。

【請求項９】

前記認証システムであって、

前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする請求項８記載の認証システム。

【請求項１０】

前記認証子システムであって、

記録媒体の代わりに通信媒体を利用することを特徴とする請求項５記載の認証システム。

【請求項１１】

コンテンツを再生する再生装置であって、

前記再生装置は、読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする再生装置。

【請求項１２】

前記再生装置であって、

前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、保持する証明書のＩＤ番号が含まれる２つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする請求項１１記載の再生装置。

【請求項１３】

コンテンツを再生する再生装置であって、

前記再生装置は、前記読出装置が読み出した第１の認証用データを受信する受信部と、前記第１の認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第２の認証用データを受信する受信部と、前記第２の認証用データの正当性を

検証する検証部と、前記検証後に前記第２の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする再生装置。

【請求項１４】

前記再生装置であって、

前記読出装置が前記再生装置を認証する前記第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、保持する証明書のＩＤ番号が含まれる２つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする請求項１３記載の再生装置。

【請求項１５】

前記再生装置であって、

前記読出装置が前記再生装置を認証する前記第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、保持する証明書のＩＤ番号と一致するＩＤ番号を前記第１の認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする請求項１３記載の再生装置。

【請求項１６】

認証用データ、並びにコンテンツを読み出す読出装置であって、

前記読出装置は、記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする読出装置。

【請求項１７】

前記読出装置であって、

前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、

前記検証部が検証する前記部分認証用データは、前記２つ以上のＩＤ番号に対する署名、あるいは認証子であることを特徴とする請求項１６記載の読出装置。

【請求項１８】

認証用データ、並びにコンテンツを読み出す読出装置であって、

前記読出装置は、前記記録媒体から読み出した第１の認証用データ、並びに第２の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする読出装置。

【請求項１９】

前記読出装置であって、

前記読出装置が前記再生装置を認証する前記第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読

出装置が保持する証明書を特定するＩＤ番号が登録され、
　前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、
　前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成され、
　前記検証部が検証する前記部分認証用データは、前記２つ以上のＩＤ番号に対する署名、あるいは認証子であることを特徴とする請求項１８記載の読出装置。
【請求項２０】
前記読出装置であって、
　前記読出装置が前記再生装置を認証する前記第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、
　前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、
　前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、
　前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成され、
　前記検証部が検証する前記部分認証用データは、前記ＩＤ番号に対する個別の署名、あるいは認証子であることを特徴とする請求項１８記載の読出装置。
【請求項２１】
認証用データを記録する記録媒体であって、
　前記記録媒体が記録する読出装置が再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、
　前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする記録媒体。
【請求項２２】
認証用データを記録する記録媒体であって、
　前記記録媒体が記録する読出装置が再生装置を認証する第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、
　前記記録媒体が記録する前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、
　前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、
　前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする記録媒体。
【請求項２３】
認証用データを記録する記録媒体であって、
　前記記録媒体が記録する読出装置が再生装置を認証する第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、
　前記記録媒体が記録する前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、
　前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、
　前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする記録媒体。
【請求項２４】
読出装置、あるいは再生装置を認証するための認証用データであって、
　前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする認証用データ。

【請求項２５】

読出装置、あるいは再生装置を認証するための認証用データであって、

前記読出装置が前記再生装置を認証する第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、

前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする認証用データ。

【請求項２６】

読出装置、あるいは再生装置を認証するための認証用データであって、

前記読出装置が前記再生装置を認証する第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、

前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、

前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする認証用データ。

【請求項２７】

認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、

前記端末装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、

前記読出装置は、前記記録媒体から読み出した認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする認証システム。

【請求項２８】

前記認証システムであって、

記録媒体の代わりに通信媒体を利用することを特徴とする請求項２７記載の認証システム。

【請求項２９】

認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、

前記端末装置は、前記読出装置が読み出した第１の認証用データを受信する受信部と、前記第１の認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第２の認証用データを受信する受信部と、前記第２の認証用データの正当性を検証する検証部と、前記検証後に前記第２の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、

前記読出装置は、前記記録媒体から読み出した第１の認証用データ、並びに第２の認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする認証システム。

【請求項３０】
前記認証システムであって、
　記録媒体の代わりに通信媒体を利用することを特徴とする請求項２９記載の認証システム。

【書類名】明細書
【発明の名称】認証システム、読出装置、再生装置、端末装置、記録媒体、及び認証用データ
【技術分野】
【０００１】
本発明は、公開鍵暗号を利用した認証システムに関するものであり、特に無効化された公開鍵証明書を特定する公開鍵証明書無効化リストを含む認証システムに関する。
【背景技術】
【０００２】
近年、インターネットの急速な広がりにより、インターネットをその通信の基盤とするシステムも増加している。例えば、インターネットを介して物品の売買を行う電子商取引もその１つである。このような、インターネットを通信の基盤とするシステムにおいては、通信相手がシステムの正当な参加者であることを確認することが必須となる。これを認証という。通信相手としては人間が機器を操作している場合や、機器が予め決められた手順で処理を行う場合があるが、以下ではこの両者を含めて機器という。そして通信相手を認証することを機器認証という。なお、機器が正当性、すなわち自分がシステムの正当な参加者であることを示すことを「証明する」といい、相手の正当性を確認することを「検証する」という。認証とは証明と検証の両方を含む言葉とする。
【０００３】
また、暗号技術には共通鍵暗号と公開鍵暗号がある。共通鍵暗号は暗号化のための鍵と復号のための鍵が同じ物である。一方、公開鍵暗号は暗号化のための鍵と復号のための鍵が異なるものである。認証を行うには公開鍵暗号を用いる方が望ましい。なぜならば、共通鍵暗号を用いた認証においては，検証者は証明者と同じ秘密を持つので、これ以降、検証者が証明者になりすます危険性がある。いわゆるパスワード方式はこれに該当する。公開鍵暗号を用いた認証においては，証明者は公開鍵暗号の秘密鍵を用いて証明し、検証者はその秘密鍵に対する公開鍵を用いて検証するのであり、公開鍵から秘密鍵は作成できないようになっているので、認証が終わった後で、検証者が証明者になりすますことができないからである。
【０００４】
なお、公開鍵暗号技術において、秘密鍵を用いて処理を行うことを署名といい、対応する公開鍵を用いてその署名の正当性を確認することを検証するという。
【０００５】
公開鍵暗号を用いた相手認証処理の例として、第１の機器が第２の機器にチャレンジデータとして乱数データを送信し、続いて、第２の機器がその乱数データに対して自分の秘密鍵で署名を行って第１の機器にレスポンスデータを返信し、最後に、返信されてきた署名文に対して、第１の機器が第２の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが当該システム内で有効なものであることが前提となる。
【０００６】
このために、当該システムにおいて認証局（Certification Authority：以下、ＣＡ）と呼ばれる機関から、各機器に対応する正しい公開鍵であることを示す（公開鍵に対する「お墨付き」となる）「公開鍵証明書」が発行されることが一般的である。公開鍵証明書は、機器の識別名や有効期限と公開鍵を結合したデータに認証局の電子署名が付与されたものであり、これを受け取った機器は、そのデータに対する認証局の電子署名の正しさを確認し、さらに相手機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認するものである。さらに、発行された公開鍵証明書のうち、システムから排除され，正当ではないとされる機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名が付与された公開鍵証明書無効化リスト（Certificate Revocation List：以下、ＣＲＬ）として発行される。

【０００７】
このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器の公開鍵証明書を入手し、入手した公開鍵証明書がＣＲＬに登録されたもの（無効化されたもの）でないことを確認した上で、上述の認証処理を行うことで、不正な相手機器との取引を回避することができる。なお、ＣＲＬの形式、実現例等は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。そのＣＲＬの実現例の一つとしては、特許文献１が開示されており、ＣＲＬ形式の一例としては、非特許文献１にISO/IEC/ITUが定めたX.509標準で定義されるＣＲＬ形式（データ構造）が開示されている。

【特許文献１】特開２００３－１１５８３８号公報
【特許文献２】特開２００２－２８１０１３号公報
【非特許文献１】山田慎一郎訳、「ディジタル署名と暗号技術」、ピアソン・エデュケーション
【非特許文献２】池野信一、小山謙二、「現代暗号理論」、電子通信学会

【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、前記従来の構成で相手の公開鍵証明書の有効性を判断する場合は、相手の公開鍵証明書がＣＲＬに記載されているか否かをチェックして判断する必要がある。このとき、ＣＲＬに登録する公開鍵証明書（無効化すべき公開鍵証明書）の数が増加すると、それに伴いＣＲＬのサイズが大きくなり、そのチェックに必要な処理時間も大きくなる。ここで、パソコンのような、ディスクからデータを読み出す読出装置（ドライブ）と読出装置を制御する装置（ホスト）の構成を考えた場合、ホストに比べて処理能力の低いドライブにおいても上記ＣＲＬのチェックを行う必要があり、ＣＲＬのサイズが大きくなるに従い、ドライブにかかる処理負荷が増加するという課題を有していた。
【０００９】
本発明は、前記従来の課題を解決するもので、パソコンのドライブとホストのように処理能力に大きな差がある場合に、処理能力の低いドライブにおけるＣＲＬチェックの負荷を軽減させる認証システムを提供することを目的とする。
【課題を解決するための手段】
【００１０】
本発明は、認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、前記再生装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、前記読出装置は、前記記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。
【００１１】
また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、保持する証明書のＩＤ番号が含まれる２つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする。
【００１２】
また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする。
【００１３】

また、本発明は、前記認証子システムであって、記録媒体の代わりに通信媒体を利用することを特徴とする。

【００１４】

また、本発明は、認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、前記再生装置は、前記読出装置が読み出した第１の認証用データを受信する受信部と、前記第１の認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第２の認証用データを受信する受信部と、前記第２の認証用データの正当性を検証する検証部と、前記検証後に前記第２の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、前記読出装置は、前記記録媒体から読み出した第１の認証用データ、並びに第２の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。

【００１５】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する前記第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、保持する証明書のＩＤ番号が含まれる２つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする。

【００１６】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【００１７】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する前記第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、保持する証明書のＩＤ番号と一致するＩＤ番号を前記第１の認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする。

【００１８】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【００１９】

また、本発明は、前記認証子システムであって、記録媒体の代わりに通信媒体を利用することを特徴とする。

【００２０】

また、本発明は、コンテンツを再生する再生装置であって、前記再生装置は、読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関

係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする。

【００２１】

また、本発明は、前記再生装置であって、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、保持する証明書のＩＤ番号が含まれる２つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする。

【００２２】

また、本発明は、コンテンツを再生する再生装置であって、前記再生装置は、前記読出装置が読み出した第１の認証用データを受信する受信部と、前記第１の認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第２の認証用データを受信する受信部と、前記第２の認証用データの正当性を検証する検証部と、前記検証後に前記第２の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする。

【００２３】

また、本発明は、前記再生装置であって、前記読出装置が前記再生装置を認証する前記第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、保持する証明書のＩＤ番号が含まれる２つ以上のＩＤ番号を前記認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする。

【００２４】

また、本発明は、前記再生装置であって、前記読出装置が前記再生装置を認証する前記第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、保持する証明書のＩＤ番号と一致するＩＤ番号を前記第１の認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置は、前記読出装置が保持する証明書のＩＤ番号が前記第２の認証用データに登録されているか否かを判定することを特徴とする。

【００２５】

また、本発明は、認証用データ、並びにコンテンツを読み出す読出装置であって、前記読出装置は、記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。

【００２６】

また、本発明は、前記読出装置であって、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、前記検証部が検証する前記部分認証用データは、前記２つ以上のＩＤ番号に対する署名、あるいは認証子であることを特徴とする。

【００２７】

また、本発明は、認証用データ、並びにコンテンツを読み出す読出装置であって、前記読出装置は、前記記録媒体から読み出した第１の認証用データ、並びに第２の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正

当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。

【００２８】

また、本発明は、前記読出装置であって、前記読出装置が前記再生装置を認証する前記第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成され、前記検証部が検証する前記部分認証用データは、前記２つ以上のＩＤ番号に対する署名、あるいは認証子であることを特徴とする。

【００２９】

また、本発明は、前記読出装置であって、前記読出装置が前記再生装置を認証する前記第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置が前記読出装置を認証する前記第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成され、前記検証部が検証する前記部分認証用データは、前記ＩＤ番号に対する個別の署名、あるいは認証子であることを特徴とする。

【００３０】

また、本発明は、認証用データを記録する記録媒体であって、前記記録媒体が記録する読出装置が再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする。

【００３１】

また、本発明は、認証用データを記録する記録媒体であって、前記記録媒体が記録する読出装置が再生装置を認証する第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記記録媒体が記録する前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【００３２】

また、本発明は、認証用データを記録する記録媒体であって、前記記録媒体が記録する読出装置が再生装置を認証する第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、前記記録媒体が記録する前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【００３３】

また、本発明は、読出装置、あるいは再生装置を認証するための認証用データであって

、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする。

【００３４】

また、本発明は、読出装置、あるいは再生装置を認証するための認証用データであって、前記読出装置が前記再生装置を認証する第１の認証用データには、無効化すべき再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、２つ以上のＩＤ番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【００３５】

また、本発明は、読出装置、あるいは再生装置を認証するための認証用データであって、前記読出装置が前記再生装置を認証する第１の認証用データには、有効な再生装置が保持する証明書を特定するＩＤ番号が登録され、前記再生装置が前記読出装置を認証する第２の認証用データには、無効化すべき読出装置が保持する証明書を特定するＩＤ番号が登録され、前記読出装置が前記再生装置を認証する第１の認証用データに登録されたＩＤ番号には、それぞれのＩＤ番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第２の認証用データに対しては、登録されたＩＤ番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【００３６】

また、本発明は、認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、前記端末装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、前記読出装置は、前記記録媒体から読み出した認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする。

【００３７】

また、本発明は、前記認証システムであって、記録媒体の代わりに通信媒体を利用することを特徴とする。

【００３８】

また、本発明は、認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、前記端末装置は、前記読出装置が読み出した第１の認証用データを受信する受信部と、前記第１の認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第２の認証用データを受信する受信部と、前記第２の認証用データの正当性を検証する検証部と、前記検証後に前記第２の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、前記読出装置は、前記記録媒体から読み出した第１の認証用データ、並びに第２の認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする。

【００３９】

また、本発明は、前記認証システムであって、記録媒体の代わりに通信媒体を利用する

ことを特徴とする。
【発明の効果】
【００４０】
本発明によれば、処理能力の高い再生装置がＣＲＬの検索を行うことで、読出装置がＣＲＬの検索を行わず、署名検証だけを実施する構成にすることが可能であり、効率のよい認証システムを実現することが可能である。また、その場合に、再生装置が検索するＣＲＬのＩＤの区間に対して署名を施す、あるいは個々のＩＤに対して署名を施すことにより、再生装置の不正行為も防止することができる。
【００４１】
また、本発明によれば、双方向認証を実施する場合、再生装置による読出装置の認証には、従来から用いられるＣＲＬを利用して再生装置がＣＲＬを検索して、逆に、読出装置による再生装置の認証であっても、再生装置がＣＲＬを検索して、読出装置は検索結果の検証を実施するだけで、再生装置の認証を実施することが可能となるため、効率的な双方向の認証システムを実現することも可能である。
【発明を実施するための最良の形態】
【００４２】
以下、本発明の実施の形態について、図面を参照しながら説明する。図１は、本発明に係る認証システムの全体構成を示すブロック図である。このシステムは、公開鍵の正当性を示す公開鍵証明書と、無効化した公開鍵証明書の一覧を示す公開鍵証明書無効化リスト（以下、ＣＲＬ）を発行する公開鍵証明書認証局（以下、ＣＡ）の端末装置１０１と、前記発行されたＣＲＬと、暗号化されたコンテンツ（以下、暗号化コンテンツ）を記録する記録媒体１０２と、前記記録媒体１０２からＣＲＬ、及び暗号化コンテンツを読み出す読出装置１０３と、前記読出装置１０３と認証を行い、前記暗号化コンテンツを復号して再生する再生装置１０４からなる。
【００４３】
ただし、ＣＡの端末装置１０１は、無効化する公開鍵証明書が発生するごとにＣＲＬを更新して記録媒体１０２に記録する、あるいは前記記録媒体１０２を製造する製造メーカに更新したＣＲＬを配布するものとする。また、読出装置１０３と再生装置１０４は、汎用の通信路で接続されており、一方が他方を認証する片方向認証、あるいは両者が互いに認証し合う相互認証を実施した後、認証結果がＯＫであれば、読出装置１０３は、暗号化コンテンツを再生装置１０４へ送信し、再生装置１０４がコンテンツの再生を行う。ここで、汎用の通信路とは、その仕様が公開されているため、通信路上のデータ盗聴、改ざん、差し替えなどの危険に晒される安全でない通信路のことである。
【００４４】
（実施の形態１）
図２は、本発明の実施の形態１における、読出装置１０３が再生装置１０４を認証する片方向認証の場合の読出装置１０３、並びに再生装置１０４の機能を示す機能ブロック図である。
【００４５】
読出装置１０３は、ＣＡの公開鍵を格納するＣＡ公開鍵格納部２０１と、前記ＣＡの公開鍵を用いてＣＡが付与した署名の正当性を検証する署名検証部２０２と、記録媒体１０２に記録されているＣＲＬと、再生装置１０４から受信したＣＲＬのバージョン番号が一致するか否かを比較する比較部２０３と、再生装置１０４から受信した証明書、並びにＣＲＬを用いて、前記証明書が有効であるか否かを判定する有効性判定部２０４と、読出装置１０３と再生装置１０４を接続する汎用通信路上で情報を安全に送信（暗号化して送信）するために必要なセッション鍵を生成するセッション鍵生成部２０５と、前記セッション鍵を再生装置１０４から受信した証明書に含まれる公開鍵で暗号化する暗号化部２０６と、記録媒体１０２に記録されている暗号化コンテンツ鍵を前記セッション鍵で暗号化する暗号化部２０７を備える。
【００４６】

再生装置１０４は、自身の証明書を格納する証明書格納部２１１と、読出装置１０３を経由して記録媒体１０２に記録されている再生装置認証用ＣＲＬを受信して、前記証明書を用いて前記再生装置認証用ＣＲＬを検索して、該当するＩＤの区間、バージョン番号、それらに対する署名を抽出する検索／抽出部２１２と、前記ＣＲＬから抽出した情報と、前記証明書を読出装置１０３へ送信する証明書／再生装置認証用ＣＲＬ送信部２１３と、再生装置１０４が保持する証明書に含まれる公開鍵に対応する秘密鍵を格納する秘密鍵格納部２１４と、読出装置１０３から受信した暗号化セッション鍵を前記秘密鍵を用いて復号する復号部２１５と、同じく読出装置１０３から受信した２重暗号化されたコンテンツ鍵を前記復号して得たセッション鍵を用いて復号する復号部２１６と、再生装置１０４が保持するデバイス鍵を格納するデバイス鍵格納部２１７と、読出装置１０３を経由して記録媒体１０２に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部２１８と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部２１９と、読出装置１０３を経由して記録媒体１０２に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵を用いて復号してコンテンツを獲得する復号部２２０を備える。

〔００４７〕

また、記録媒体１０２には、暗号化メディア鍵２３１、再生装置認証用ＣＲＬ２３２、暗号化コンテンツ鍵２３３、暗号化コンテンツ２３４が記録されている。

〔００４８〕

なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献２が開示されている。

【００４９】

次に、記録媒体１０２に記録される各種データのデータ形式について、図３を用いて説明する。

【００５０】

記録媒体１０２は、再生装置用ＣＲＬを記録する再生装置用ＣＲＬ記録領域３０１と、暗号化メディア鍵を記録する暗号化メディア鍵記録領域３０２と、暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域３０３と、暗号化コンテンツを記録する暗号化コンテンツ記録領域３０４を備える。

【００５１】

再生装置認証用ＣＲＬは、バージョン番号（ＶＮ）、無効化する証明書のＩＤ（ＲＩＤ）、及びそれらの正当性を証明するＣＡの署名により構成される。図３は、３番のＩＤを持つ証明書と１０番のＩＤを持つ証明書が無効化されている場合の例を示している。このとき、実際の証明書には割り当てない０番と９９９９番のＩＤも合わせてＣＲＬに対して記録される。また、バージョン番号は、ＣＲＬが更新された場合に１ずつカウントアップされる値である。さらに、ＣＡの署名は、バージョン番号と連続する証明書のＩＤを連結した値に対して付与される。ただし、記号「||」は、データを連結することを意味する記号として用い、関数Sig（X, Y）は、データＹに対して、鍵データＸを用いて署名生成を行う関数として用いる。また、ＳＫ__ＣＡはＣＡだけが保持する署名生成に利用する秘密鍵のことである。

【００５２】

暗号化メディア鍵は、ある特定の装置にだけメディア鍵を与えるためのデータであり、メディア鍵を与える装置が持つデバイス鍵（ＤＫ）ではメディア鍵（Ｋｍ）を暗号化して、メディア鍵を与えない装置が持つデバイス鍵（ＤＫ）ではメディア鍵とは全く無関係なダミーデータを暗号化する。図３は、ＤＫ３を持つ装置と、ＤＫ１０を持つ装置に対してはメディア鍵を与えない場合の例を示している。ただし、関数E（X, Y）は、データＹを鍵データＸを用いて暗号化する関数として用いる。

【００５３】

暗号化コンテンツ鍵は、前記メディア鍵で暗号化されたコンテンツ鍵であり、暗号化コ

ンテンツは前記コンテンツ鍵で暗号化されたコンテンツである。

【００５４】

次に、図４～図６を用いて、読出装置１０３と再生装置１０４の動作について説明する。

【００５５】

Ｓ４０１：再生装置１０４は、読出装置１０３を経由して記録媒体１０２から再生装置認証用ＣＲＬを受信する。

【００５６】

Ｓ４０２：再生装置１０４は、受信したＣＲＬから、自身が保持する証明書のＩＤが含まれる区間を検索して、区間、ＣＲＬのバージョン番号、及びそれらに対する署名を抽出する。例えば、図３に示す記録媒体１０２の場合、再生装置１０４が保持する証明書のＩＤが５番であれば、ＣＲＬのバージョン番号　VN=0001、区間　RID2=0003～RID3=0010、及びそれらに対する署名　Sig（SK_CA, VN||RID2||RID3）を抽出する。また、再生装置１０４が保持する証明書のＩＤが３番であれば、ＣＲＬのバージョン番号　VN=0001、区間　RID1=0000～RID2=0003、もしくはRID2=0003～RID3=0005、及びそれらに対する署名　Sig（SK_CA, VN||RID1||RID2）、もしくはSig（SK_CA, VN||RID2||RID3）を抽出する。

【００５７】

Ｓ４０３：再生装置１０４は、Ｓ４０２で抽出した各種データ、及び保持する証明書を読出装置１０３へ送信する。

【００５８】

Ｓ４０４：読出装置１０３は、再生装置１０４から受信した証明書、及び署名を、保持するＣＡの公開鍵を用いて検証する。

【００５９】

Ｓ４０５：Ｓ４０４で検証を実行した結果、検証ＯＫであればＳ５０１へ、検証ＮＧであれば処理を中止する。

【００６０】

Ｓ５０１：読出装置１０３は、再生装置１０４から受信したＣＲＬのバージョン番号と、記録媒体１０２に記録されているバージョン番号が一致するか否かを比較する。

【００６１】

Ｓ５０２：Ｓ５０１で比較を実行した結果、一致であればＳ５０３へ、不一致であれば処理を中止する。

【００６２】

Ｓ５０３：読出装置１０３は、Ｓ４０４、並びにＳ５０１で検証／比較した再生装置１０４の証明書、並びに再生装置１０４により抽出されたＣＲＬの一部を用いて、証明書が有効か否かを判定する。例えば、ＩＤが５番の証明書を保持する再生装置１０４が、区間　RID2=0003～RID3=0010を送信してきた場合は、値５は区間３～１０（4, 5, 6, 7, 8, 9）に含まれるためその証明書を有効と判断する。また、ＩＤが３番の証明書を保持する再生装置１０４が、区間　RID2=0003～RID3=0010を送信してきた場合は、値３は区間３～１０には含まれないためその証明書を無効と判断する。

【００６３】

Ｓ５０４：Ｓ５０３で判定を実行した結果、有効であればＳ５０５へ、無効であれば処理を中止する。

【００６４】

Ｓ５０５：読出装置１０３は、汎用通信路上でデータを安全に送信（暗号化して送信）するためのセッション鍵を生成して、再生装置１０４から受信した証明書に含まれる公開鍵を用いて暗号化して再生装置１０４へ送信する。

【００６５】

Ｓ５０６：再生装置１０４は、読出装置１０３から受信した暗号化セッション鍵を、証明書に含まれる公開鍵に対応する秘密鍵で復号してセッション鍵を得る。

【００６６】

Ｓ６０１：読出装置１０３は、Ｓ５０５で生成したセッション鍵を用いて、記録媒体１０２に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置１０４へ送信する。

【００６７】

Ｓ６０２：再生装置１０４は、読出装置１０３から受信した２重暗号化されたコンテンツ鍵を、Ｓ５０６で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。

【００６８】

Ｓ６０３：再生装置１０４は、読出装置１０３を経由して記録媒体１０２から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、Ｓ６０２で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。

【００６９】

Ｓ６０４：再生装置１０４は、読出装置１０３を経由して記録媒体１０２から暗号化コンテンツを受信して、Ｓ６０３で得たコンテンツ鍵で復号してコンテンツを得る。

【００７０】

以上に示したように、従来では、読出装置が再生装置を認証する場合、読出装置がＣＲＬを検索しなければならないが、本発明の構成では、読出装置はＣＲＬの検索を行わず、再生装置が検索したＣＲＬの確認（検証）を実行するだけでよく、処理能力の低い読取装置であっても認証処理を効率的に行うことが可能となる。

【００７１】

（実施の形態２）

図７は、本発明の実施の形態２における、読出装置７００と再生装置７２０が相互認証を実行する場合の読出装置７００、並びに再生装置７２０の機能を示す機能ブロック図である。

【００７２】

読出装置７００は、ＣＡの公開鍵を格納するＣＡ公開鍵格納部７０１と、前記ＣＡの公開鍵を用いてＣＡが付与した署名の正当性を検証する署名検証部７０２と、記録媒体７４０に記録されているＣＲＬと、再生装置７２０から受信したＣＲＬのバージョン番号が一致するか否かを比較する比較部７０３と、再生装置７２０から受信した証明書、並びにＣＲＬを用いて、前記証明書が有効であるか否かを判定する有効性判定部７０４と、自身の証明書を格納する証明書格納部７０５と、前記証明書を再生装置７２０へ送信する証明書送信部７０６と、読出装置１０３と再生装置１０４を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Secure Authentication Channel：SAC）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部７０７と、記録媒体７４０に記録されている暗号化コンテンツを前記処理で共有したセッション鍵で暗号化する暗号化部７０８を備える。

【００７３】

再生装置７２０は、自身の証明書を格納する証明書格納部７２１と、読出装置７００を経由して記録媒体７４０に記録されている再生装置認証用ＣＲＬを受信して、前記証明書を用いて前記再生装置認証用ＣＲＬを検索して、該当するＩＤの区間、バージョン番号、それらに対する署名を抽出する検索／抽出部７２２と、前記ＣＲＬから抽出した情報と、前記証明書を読出装置７００へ送信する証明書／再生装置認証用ＣＲＬ送信部７２３と、ＣＡの公開鍵を格納するＣＡ公開鍵格納部７２４と、前記ＣＡの公開鍵を用いてＣＡが付与した署名の正当性を検証する署名検証部７２５と、読出装置７００から受信した証明書、並びに読出装置７００を経由して記録媒体７４０から受信した読出装置認証用ＣＲＬを用いて、前記証明書が有効であるか否かを判定する有効性判定部７２６と、再生装置７２０と読出装置７００を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Secure Authentication Channel：SAC）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部７２７と、読出装置７００から受信した２重暗号化されたコンテンツ鍵を前記処理で共有したセッション鍵で復号する復号部７２８と、再生装置７２０が保持するデバイス鍵を格納するデバイス鍵格納部７２９と、読出装置７００を経由して

記録媒体７４０に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部７３０と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部７３１と、読出装置７００を経由して記録媒体７４０に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵で復号してコンテンツを獲得する復号部７３２を備える。

【００７４】

また、記録媒体７４０には、暗号化メディア鍵７４１、再生装置認証用ＣＲＬ７４２、読出装置認証用ＣＲＬ７４３、暗号化コンテンツ鍵７４４、暗号化コンテンツ７４５が記録されている。

【００７５】

なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献２が開示されている。

【００７６】

次に、記録媒体７４０に記録される各種データのデータ形式について、図８を用いて説明する。

【００７７】

記録媒体７４０は、再生装置認証用ＣＲＬを記録する再生装置認証用ＣＲＬ記録領域８０１と、読出装置認証用ＣＲＬを記録する読出装置認証用ＣＲＬ記録領域８０２と、暗号化メディア鍵を記録する暗号化メディア鍵記録領域８０３と、暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域８０４と、暗号化コンテンツを記録する暗号化コンテンツ記録領域８０５を備える。

【００７８】

再生装置認証用ＣＲＬは、バージョン番号（ＶＮ）、無効化する証明書のＩＤ（ＲＩＤ）、及びそれらの正当性を証明するＣＡの署名により構成される。図８は、３番のＩＤを持つ証明書と１０番のＩＤを持つ証明書が無効化されている場合の例を示している。このとき、実際の証明書には割り当てない０番と９９９９番のＩＤも合わせてＣＲＬに対して記録される。また、バージョン番号は、ＣＲＬが更新された場合に１ずつカウントアップされる値である。さらに、ＣＡの署名は、バージョン番号と連続する証明書のＩＤを連結した値に対して付与される。

【００７９】

読出装置認証用ＣＲＬは、バージョン番号（ＶＮ’）、無効化する証明書のＩＤ（ＲＩＤ’）、及びそれら全体の正当性を証明するＣＡの署名により構成される。図８は、１番のＩＤを持つ証明書、６番のＩＤを持つ証明書、及び１５番のＩＤを持つ証明書が無効化されている場合の例を示している。

【００８０】

暗号化メディア鍵は、ある特定の装置にだけメディア鍵を与えるためのデータであり、メディア鍵を与える装置が持つデバイス鍵（ＤＫ）ではメディア鍵（Ｋｍ）を暗号化して、メディア鍵を与えない装置が持つデバイス鍵（ＤＫ）ではメディア鍵とは全く無関係なダミーデータを暗号化する。図８は、ＤＫ３を持つ装置と、ＤＫ１０を持つ装置に対してはメディア鍵を与えない場合の例を示している。

【００８１】

暗号化コンテンツ鍵は、前記メディア鍵で暗号化されたコンテンツ鍵であり、暗号化コンテンツは前記コンテンツ鍵で暗号化されたコンテンツである。

【００８２】

次に、図９～図１２を用いて、読出装置７００と再生装置７２０の動作について説明する。

【００８３】

Ｓ９０１：再生装置７２０は、読出装置７００を経由して記録媒体７４０から再生装置認証用ＣＲＬを受信する。

【００８４】
Ｓ９０２：再生装置７２０は、受信したＣＲＬから、自身が保持する証明書のＩＤが含まれる区間を検索して、区間、ＣＲＬのバージョン番号、及びそれらに対する署名を抽出する。例えば、図８に示す記録媒体７４０の場合、再生装置７２０が保持する証明書のＩＤが５番であれば、ＣＲＬのバージョン番号　VN=0001、区間　RID2=0003～RID3=0010、及びそれらに対する署名　Sig（SK_CA, VN||RID2||RID3）を抽出する。また、再生装置７２０が保持する証明書のＩＤが３番であれば、ＣＲＬのバージョン番号　VN=0001、区間　RID1=0000～RID2=0003、もしくはRID2=0003～RID3=0005、及びそれらに対する署名　Sig（SK_CA, VN||RID1||RID2）、もしくはSig（SK_CA, VN||RID2||RID3）を抽出する。
【００８５】
Ｓ９０３：再生装置７２０は、Ｓ９０２で抽出した各種データ、及び保持する証明書を読出装置７００へ送信する。
【００８６】
Ｓ９０４：読出装置７００は、再生装置７２０から受信した証明書、及び署名を、保持するＣＡの公開鍵を用いて検証する。
【００８７】
Ｓ９０５：Ｓ９０４で検証を実行した結果、検証ＯＫであればＳ１００１へ、検証ＮＧであれば処理を中止する。
【００８８】
Ｓ１００１：読出装置７００は、再生装置７２０から受信したＣＲＬのバージョン番号と、記録媒体７４０に記録されているバージョン番号が一致するか否かを比較する。
【００８９】
Ｓ１００２：Ｓ１００１で比較を実行した結果、一致であればＳ１００３へ、不一致であれば処理を中止する。
【００９０】
Ｓ１００３：読出装置７００は、Ｓ９０４、並びにＳ１００１で検証／比較した再生装置７２０の証明書、並びに再生装置７２０により抽出されたＣＲＬの一部を用いて、証明書が有効か否かを判定する。例えば、ＩＤが５番の証明書を保持する再生装置７２０が、区間　RID2=0003～RID3=0010を送信してきた場合は、値５は区間３～１０（4, 5, 6, 7, 8, 9）に含まれるためその証明書を有効と判断する。また、ＩＤが３番の証明書を保持する再生装置７２０が、区間　RID2=0003～RID3=0010を送信してきた場合は、値３は区間３～１０には含まれないためその証明書を無効と判断する。
【００９１】
Ｓ１００４：Ｓ１００３で判定を実行した結果、有効であればＳ１００５へ、無効であれば処理を中止する。
【００９２】
Ｓ１００５：読出装置７００は、保持する自身の証明書を再生装置７４０へ送信する。
【００９３】
Ｓ１１０１：再生装置７２０は、読出装置７００から受信した証明書、及び読出装置７００を経由して記録媒体７４０から受信した読出装置認証用ＣＲＬに付与されている署名をＣＡの公開鍵を用いて検証する。
【００９４】
Ｓ１１０２：Ｓ１１０１で検証を実行した結果、検証ＯＫであればＳ１１０３へ、検証ＮＧであれば処理を中止する。
【００９５】
Ｓ１１０３：再生装置７２０は、受信した証明書、並びに読出装置認証用ＣＲＬを用いて、証明書が有効か否かを判定する。例えば、ＩＤが５番の証明書を保持する読出装置７００が、読出装置認証用ＣＲＬを送信してきた場合は、値５は受信したＣＲＬに登録されていないためその証明書を有効と判断する。また、ＩＤが６番の証明書を保持する読出装置７００が、読出装置認証用ＣＲＬを送信してきた場合は、値６は受信したＣＲＬに登録

されているためその証明書を無効と判断する。

【００９６】

Ｓ１１０４：Ｓ１１０３で判定を実行した結果、有効であればＳ１１０５／Ｓ１１０６へ、無効であれば処理を中止する。

【００９７】

Ｓ１１０５／Ｓ１１０６：読出装置７００と再生装置７２０の間では、両者の公開鍵暗号化処理部が動作してＳＡＣを確立し、データの受け渡しはＳＡＣを介して安全に行われる。このＳＡＣの実現方法については、後に詳細を述べる。ＳＡＣ処理の結果として、両者はセッション鍵を共有する。

【００９８】

Ｓ１２０１：読出装置７００は、Ｓ１１０６で生成したセッション鍵を用いて、記録媒体７４０に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置７２０へ送信する。

【００９９】

Ｓ１２０２：再生装置７２０は、読出装置７００から受信した２重暗号化されたコンテンツ鍵を、Ｓ１１０５で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。

【０１００】

Ｓ１２０３：再生装置７２０は、読出装置７００を経由して記録媒体７４０から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、Ｓ１２０２で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。

【０１０１】

Ｓ１２０４：再生装置７２０は、読出装置７００を経由して記録媒体７４０から暗号化コンテンツを受信して、Ｓ１２０３で得たコンテンツ鍵で復号してコンテンツを得る。

【０１０２】

以上に示したように、従来では、読出装置と再生装置が相互認証を実行する場合、読出装置もＣＲＬを検索しなければならないが、本発明の構成では、読出装置が再生装置を認証する場合は、読出装置はＣＲＬの検索を行わず、再生装置が検索したＣＲＬの確認（検証）を実行するだけでよく、逆に、再生装置が読出装置を認証する場合もまた、再生装置がＣＲＬの検索を行うため、処理能力の低い読取装置であっても相互認証処理を効率的に行うことが可能となる。

【０１０３】

次に、読出装置７００と再生装置７２０との間で設定されるＳＡＣの実現方法について図１３を用いて説明する。ただし、Sign( )を署名生成関数、Veri( )を署名検証関数、Gen( )を鍵生成関数とし、Ｙをそのシステム固有のシステムパラメータとする。また、鍵生成関数Gen( )は、Gen(x,Gen(y,z)) = Gen(y,Gen(x,z))の関係を満たすものとする。なお、このような鍵生成関数は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、非特許文献２に、ディフィ-ヘルマン（ＤＨ）型公開鍵配送法が開示されている。

【０１０４】

Ｓ１３０１：読出装置Ａは、ＣＡが発行した証明書Ｃｅｒｔ＿Ａを再生装置Ｂに送信する。ここでは、証明書の構成要素は、Ａの公開鍵ＰＫ＿Ａ、ＡのＩＤ（ＩＤ＿Ａ）、それらに対するＣＡの署名Ｓｉｇ＿ＣＡとしている。

【０１０５】

Ｓ１３０２：再生装置Ｂは、ＣＡの公開鍵Ｐ＿ＣＡを用いてＣｅｒｔ＿Ａに付与されている署名Ｓｉｇ＿ＣＡが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。さらに、再生装置Ｂは、読出装置ＡのＩＤ（ＩＤ＿Ａ）が、ＣＲＬに登録されているか否かを確認する。登録されている場合も、ＳＡＣの設定処理を終了する。

【０１０６】

Ｓ１３０３：再生装置Ｂは、ＣＡが発行した証明書Ｃｅｒｔ＿Ｂを読出装置Ａに送信す

る。ここでは、証明書の構成要素は、Ｂの公開鍵ＰＫ＿Ｂ、ＢのＩＤ（ＩＤ＿Ｂ）、それらに対するＣＡの署名Ｓｉｇ＿ＣＡとしている。

【０１０７】

Ｓ１３０４：読出装置Ａは、ＣＡの公開鍵Ｐ＿ＣＡを用いてＣｅｒｔ＿Ｂに付与されている署名Ｓｉｇ＿ＣＡが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。さらに、読出装置Ａは、再生装置ＢのＩＤ（ＩＤ＿Ｂ）が、ＣＲＬに登録されているか否かを確認する。登録されている場合も、ＳＡＣの設定処理を終了する。

【０１０８】

Ｓ１３０５：読出装置Ａは、乱数Ｃｈａ＿Ａを生成して、再生装置Ｂに送信する。

【０１０９】

Ｓ１３０６：再生装置Ｂは、受信したＣｈａ＿Ａに対して、自身の秘密鍵ＳＫ＿Ｂで署名Ｓｉｇ＿Ｂを生成して、読出装置Ａに送信する。

【０１１０】

Ｓ１３０７：読出装置Ａは、Ｓ１３０３で受信した再生装置Ｂの公開鍵ＰＫ＿Ｂを用いて、Ｓｉｇ＿Ｂが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。

【０１１１】

Ｓ１３０８：再生装置Ｂは、乱数Ｃｈａ＿Ｂを生成して、読出装置Ａに送信する。

【０１１２】

Ｓ１３０９：読出装置Ａは、受信したＣｈａ＿Ｂに対して、自身の秘密鍵ＳＫ＿Ａで署名Ｓｉｇ＿Ａを生成して、再生装置Ｂに送信する。

【０１１３】

Ｓ１３１０：再生装置Ｂは、Ｓ１３０１で受信した読出装置Ａの公開鍵ＰＫ＿Ａを用いて、Ｓｉｇ＿Ａが正しいか否かを検証する。検証結果が正しくない場合、ＳＡＣの設定処理を終了する。

【０１１４】

Ｓ１３１１：再生装置Ｂは、乱数ｂを生成し、Key_B=Gen(b,Y)を計算して読出装置Ａに送信する。

【０１１５】

Ｓ１３１２：読出装置Ａは、乱数ａを生成し、Key_A=Gen(a,Y)を計算して再生装置Ｂに送信する。さらに、読出装置Ａは、両者で共有する鍵Key_AB=Gen(b,Key_A)を算出する。

【０１１６】

Ｓ１３１３：再生装置Ｂは、両者で共有する鍵Key_AB=Gen(a,Key_B)を算出する。

【０１１７】

（その他の変形例）

（１）本発明の実施の形態１、及び実施の形態２では、再生装置認証用ＣＲＬのデータ形式を、無効化する証明書のＩＤを記載する際、その先頭を最後にダミーのＩＤを設けてＩＤの区間に対して署名を生成する形態としたが、本発明はその構成に限定されるものではない。例えば、図１４に示すような再生装置認証用ＣＲＬの構成であってもよい。図１４の再生装置認証用ＣＲＬは、ダミーのＩＤは設けずに、先頭のＩＤに対しては、そのＩＤ単独に署名を施し、以降はＩＤの区間に対して署名を施す。そして、最後のＩＤに対しても、そのＩＤ単独に署名を施す。このような構成にすることで、読出装置が再生装置の証明書の有効性を確認できるという効果を残しつつ、再生装置認証用ＣＲＬのサイズを小さくすることが可能となる。

【０１１８】

（２）本発明の実施の形態１、及び実施の形態２では、再生装置認証用ＣＲＬを利用して読出装置が再生装置を認証する形態としたが、本発明はその構成に限定されるものではない。例えば、図１５に示すような再生装置認証用リストを利用して認証する構成であってもよい。図１５の再生装置認証用リストは、無効化すべき証明書のＩＤではなく、有効

な証明書のＩＤをリストに登録して、バージョン番号と各有効なＩＤを連結したデータに対して署名を施したものである。再生装置は、前記再生装置認証用リストを検索して、自身が保持する証明書のＩＤと一致するＩＤを抽出して、バージョン番号、抽出したＩＤ、それらに対する署名を読出装置へ送信する。読出装置は、受信した署名を検証する。

【０１１９】

（３）本発明の実施の形態１、及び実施の形態２では、記録媒体には予め暗号化されたコンテンツが記録されているＤＶＤ－Ｖｉｄｅｏのようなプリレコーディッドメディアの形態としたが、本発明はその構成に限定されるものではない。例えば、ＤＶＤ－ＲＡＭのようなレコーダブルメディアであってもよい。その場合、実施の形態１、及び実施の形態２と同様に認証を実行した後で、暗号化されたコンテンツを記録する形態となる。

【０１２０】

（４）本発明の実施の形態１、及び実施の形態２では、認証に用いるデータ、及びコンテンツが記録媒体に記録される形態としたが、本発明はその構成に限定されるものではない。記録媒体の代わりに通信媒体を利用して、通信媒体を介して、認証に用いるデータ、及びコンテンツを受け渡しする構成であってもよい。また、記録媒体、並びに通信媒体を併用する形態であってもよい。

【０１２１】

（５）本発明の実施の形態１、及び実施の形態２では、認証に用いるデータの保護にＣＡの署名を用いる形態としたが本発明はその構成に限定されるものではない。例えば、読出装置は読出装置専用の秘密鍵を保持し、再生装置は再生装置専用の秘密鍵を用いる構成として、認証に用いるデータには、各秘密鍵を利用して生成された認証子を付与する構成であってもよい。

【産業上の利用可能性】

【０１２２】

本発明にかかる認証システムは、処理能力の低い読出装置等が含まれる認証システムであっても、効率的な認証を実現できるという効果を有し、公開鍵暗号を利用した認証システムにおいて、特に無効化された公開鍵証明書を特定する公開鍵証明書無効化リストを含む認証システム等において有用である。

【図面の簡単な説明】

【０１２３】

【図１】本発明に係る認証システムの全体構成を示すブロック図
【図２】本発明の実施の形態１における機能ブロック図
【図３】本発明の実施の形態１における記録媒体に記録されるデータの例を示す図
【図４】本発明の実施の形態１における動作を示す図
【図５】本発明の実施の形態１における動作を示す図
【図６】本発明の実施の形態１における動作を示す図
【図７】本発明の実施の形態２における機能ブロック図
【図８】本発明の実施の形態２における記録媒体に記録されるデータの例を示す図
【図９】本発明の実施の形態２における動作を示す図
【図１０】本発明の実施の形態２における動作を示す図
【図１１】本発明の実施の形態２における動作を示す図
【図１２】本発明の実施の形態２における動作を示す図
【図１３】本発明の実施の形態２における相互認証の例を示す図
【図１４】本発明に係る認証システムにおける記録媒体に記録されるデータの例を示す図
【図１５】本発明に係る認証システムにおける記録媒体に記録されるデータの例を示す図

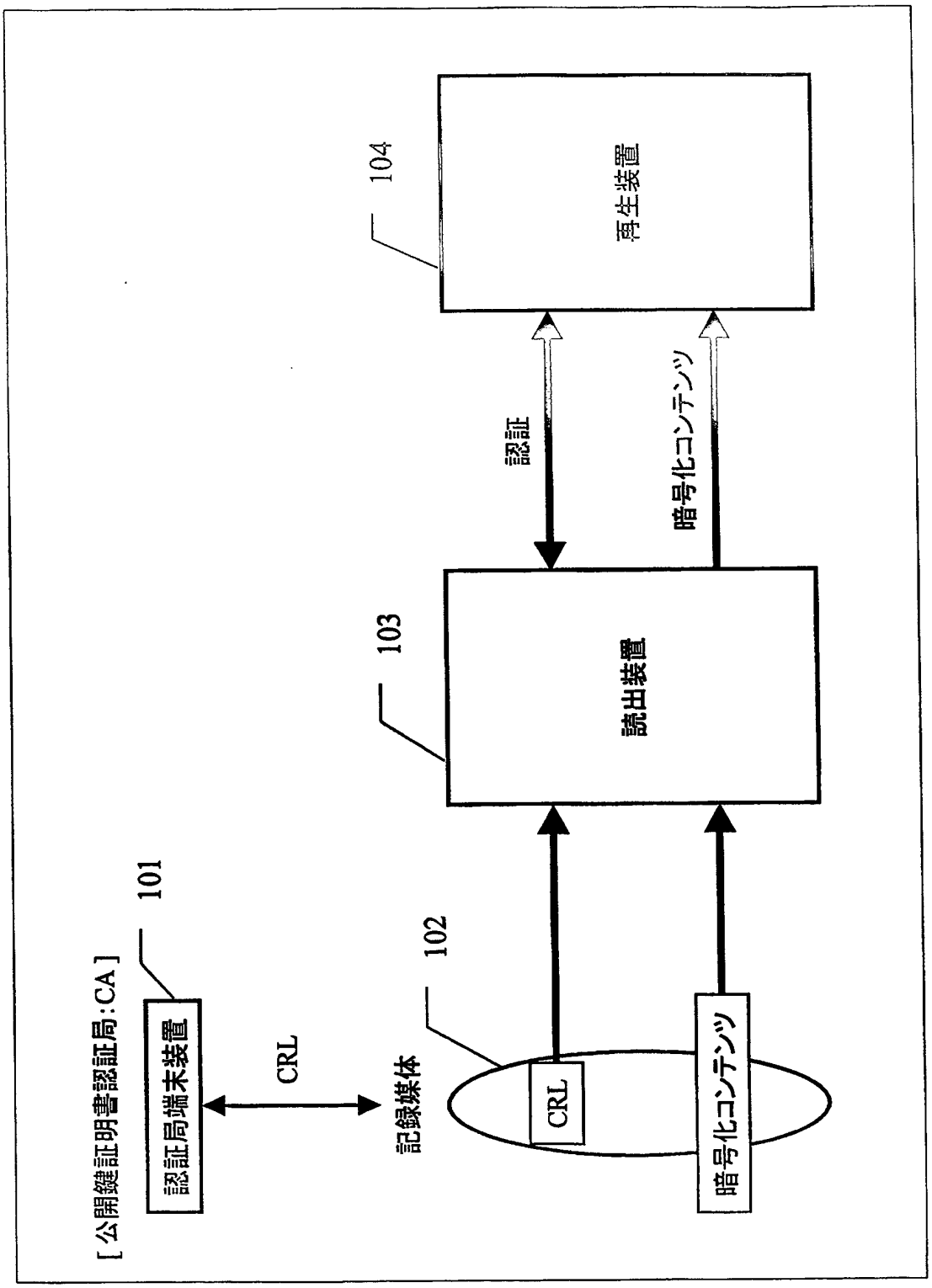
【符号の説明】

【０１２４】

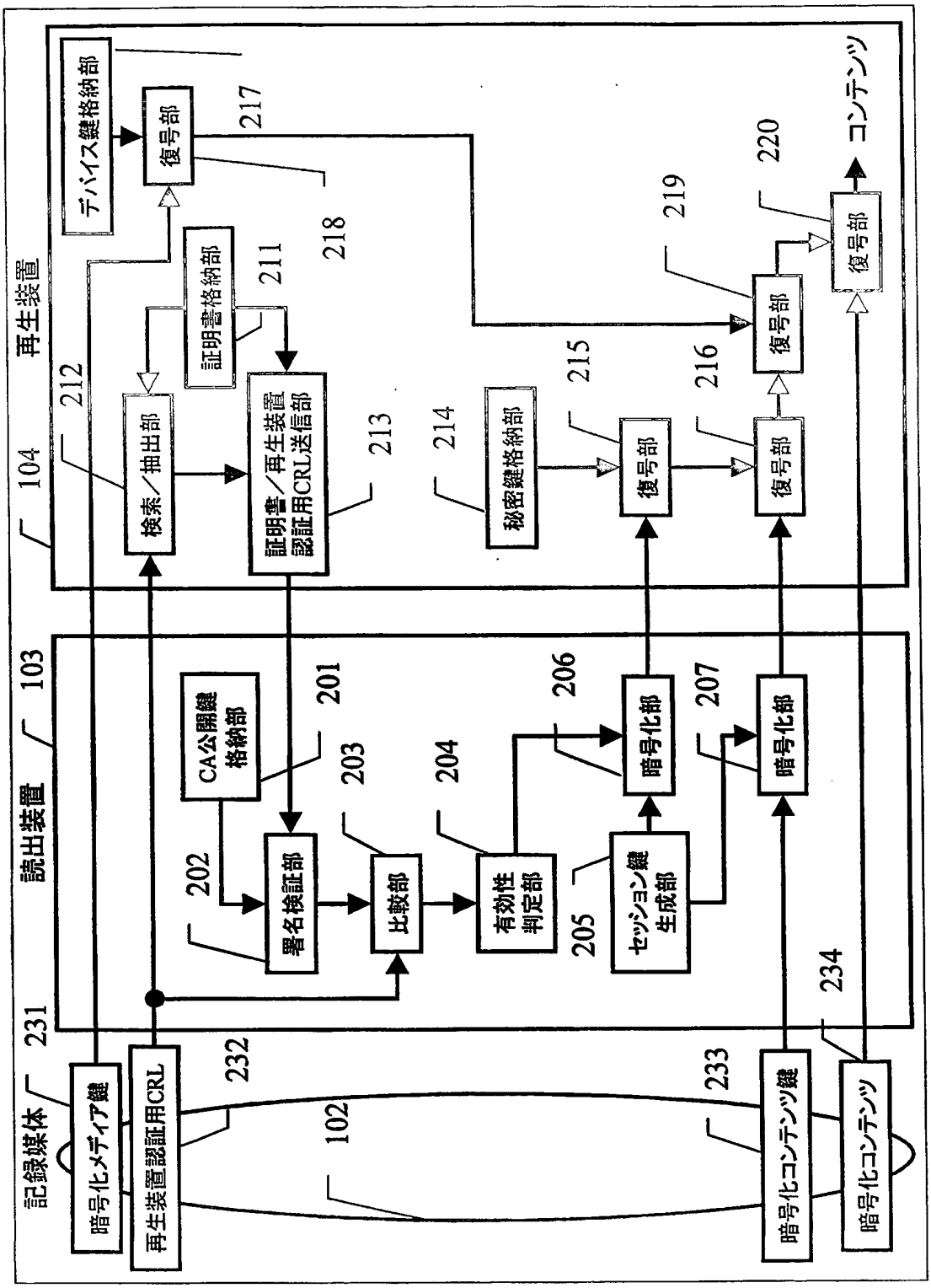
１０１　認証局端末装置

１０２　記録媒体
１０３　読出装置
１０４　再生装置

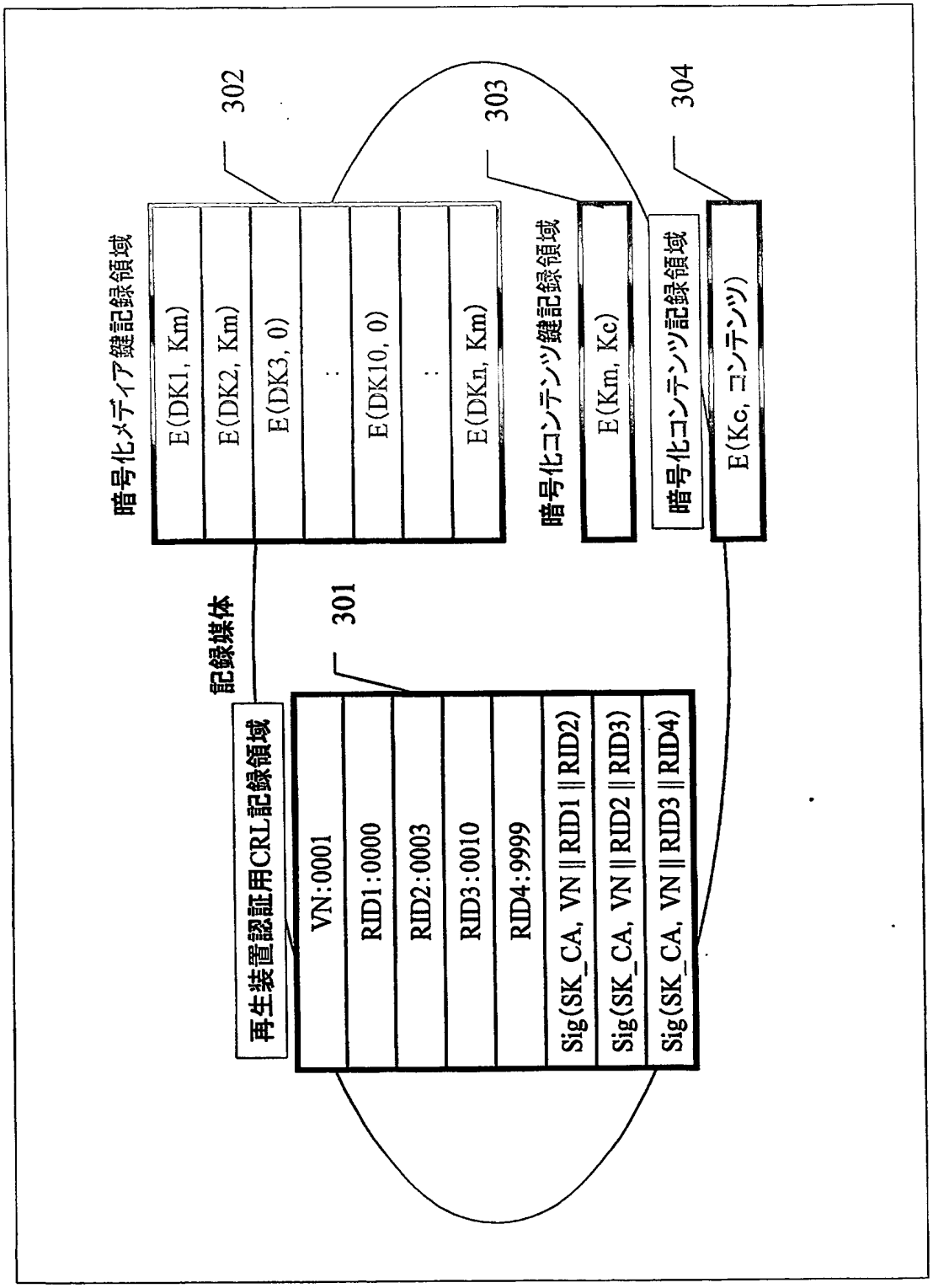
【書類名】図面
【図１】


[公開鍵証明書認証局:CA]
101
認証局端末装置
CRL
102
記録媒体
CRL
暗号化コンテンツ
103
読出装置
認証
暗号化コンテンツ
104
再生装置

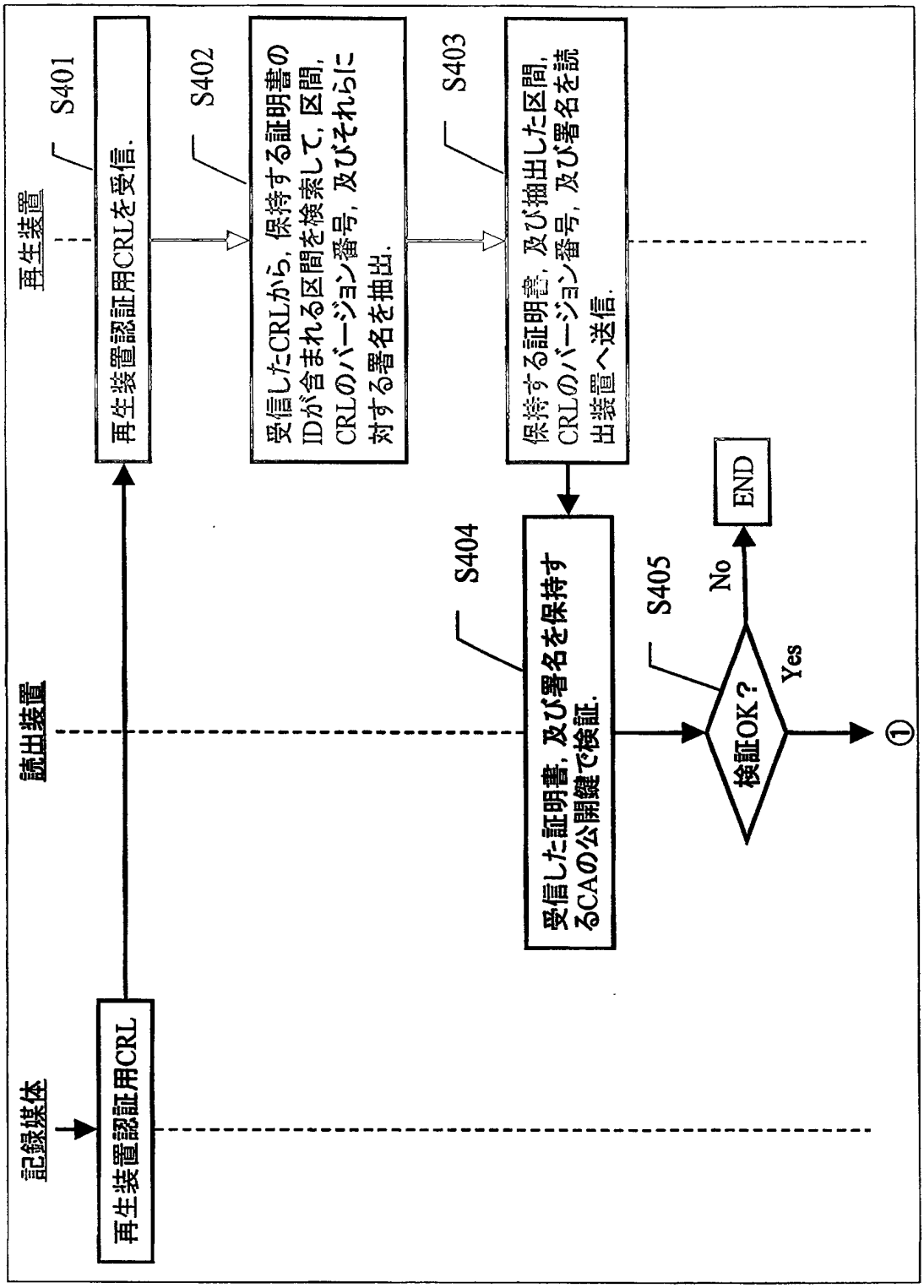
【図２】


再生装置
104
読出装置
103
記録媒体
102
暗号化メディア鍵
231
再生装置認証用CRL
232
デバイス鍵格納部
復号部
217
証明書格納部
211
218
検索／抽出部
212
証明書／再生装置認証用CRL送信部
213
秘密鍵格納部
214
215
復号部
216
復号部
219
220
復号部
コンテンツ
CA公開鍵格納部
201
署名検証部
202
203
比較部
204
有効性判定部
205
206
暗号化部
セッション鍵生成部
207
暗号化部
暗号化コンテンツ鍵
233
暗号化コンテンツ
234

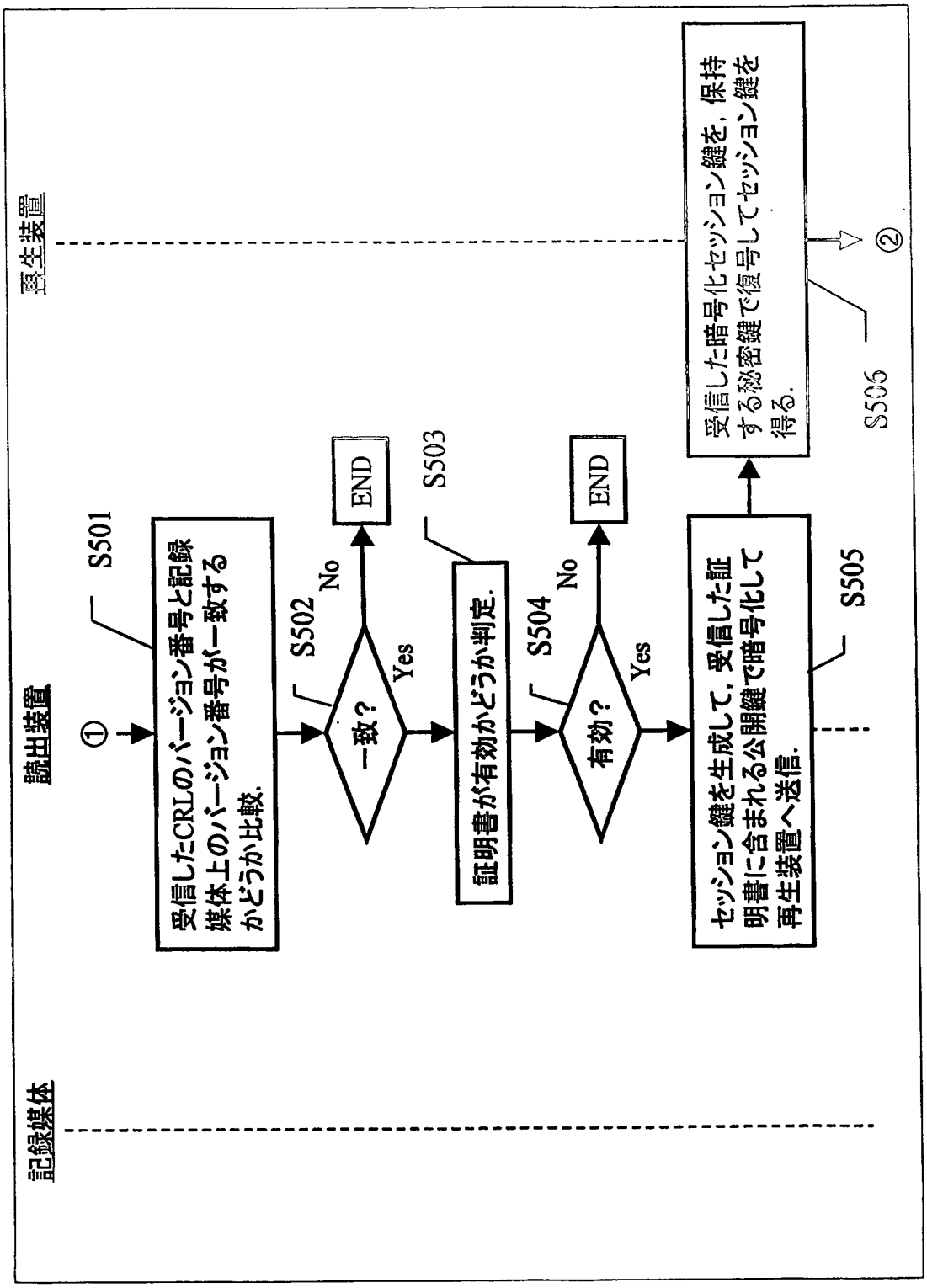
【図３】


記録媒体
再生装置認証用CRL記録領域
301
VN:0001
RID1:0000
RID2:0003
RID3:0010
RID4:9999
Sig(SK_CA, VN || RID1 || RID2)
Sig(SK_CA, VN || RID2 || RID3)
Sig(SK_CA, VN || RID3 || RID4)
暗号化メディア鍵記録領域
302
E(DK1, Km)
E(DK2, Km)
E(DK3, 0)
E(DK10, 0)
E(DKn, Km)
暗号化コンテンツ鍵記録領域
303
E(Km, Kc)
暗号化コンテンツ記録領域
304
E(Kc, コンテンツ)

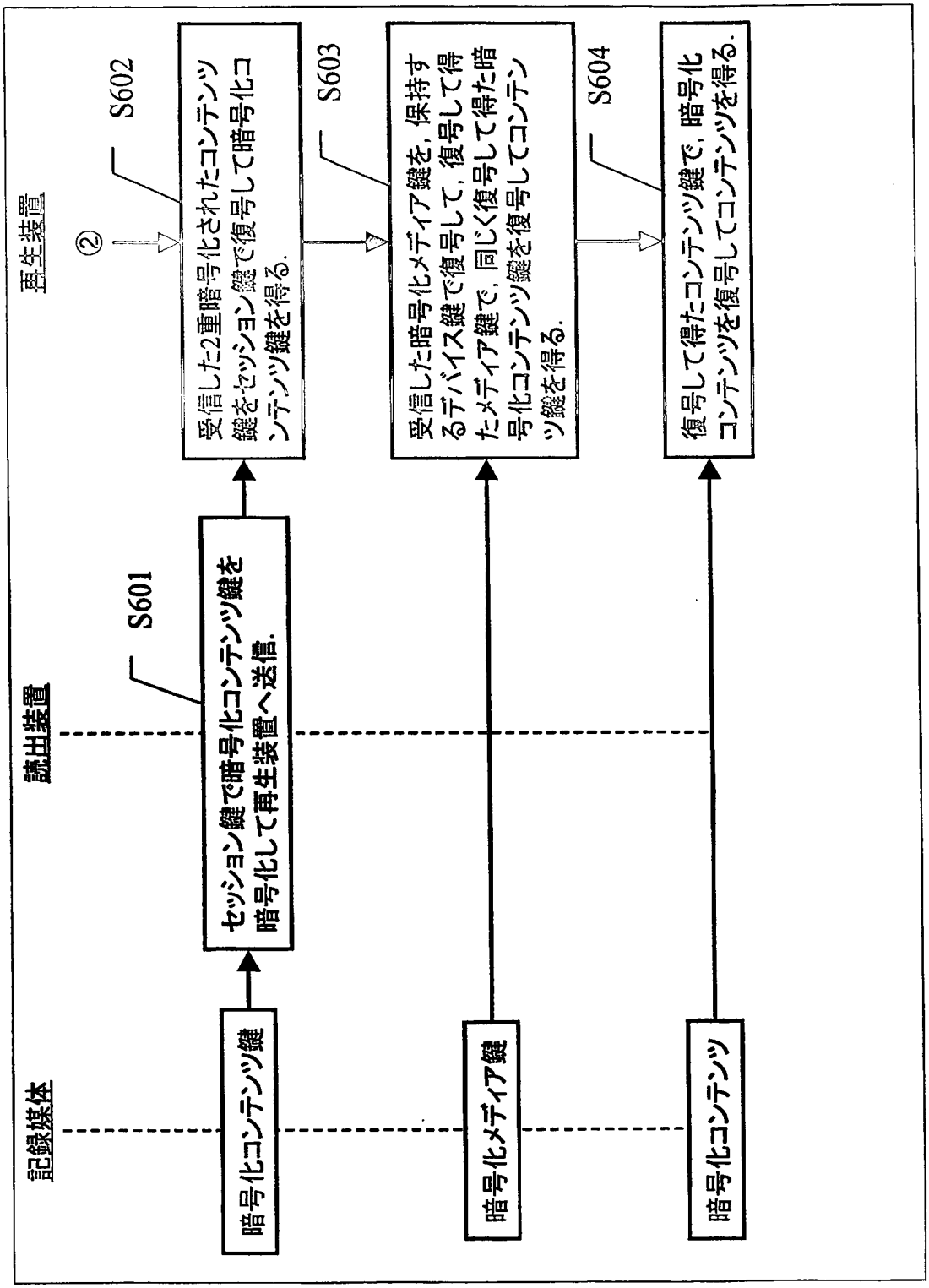
【図４】


記録媒体
再生装置認証用CRL
読出装置
再生装置
再生装置認証用CRLを受信.
S401
受信したCRLから，保持する証明書のIDが含まれる区間を検索して，区間，CRLのバージョン番号，及びそれらに対する署名を抽出.
S402
保持する証明書，及び抽出した区間，CRLのバージョン番号，及び署名を読出装置へ送信.
S403
受信した証明書，及び署名を保持するCAの公開鍵で検証.
S404
検証OK？
S405
No
Yes
END
①

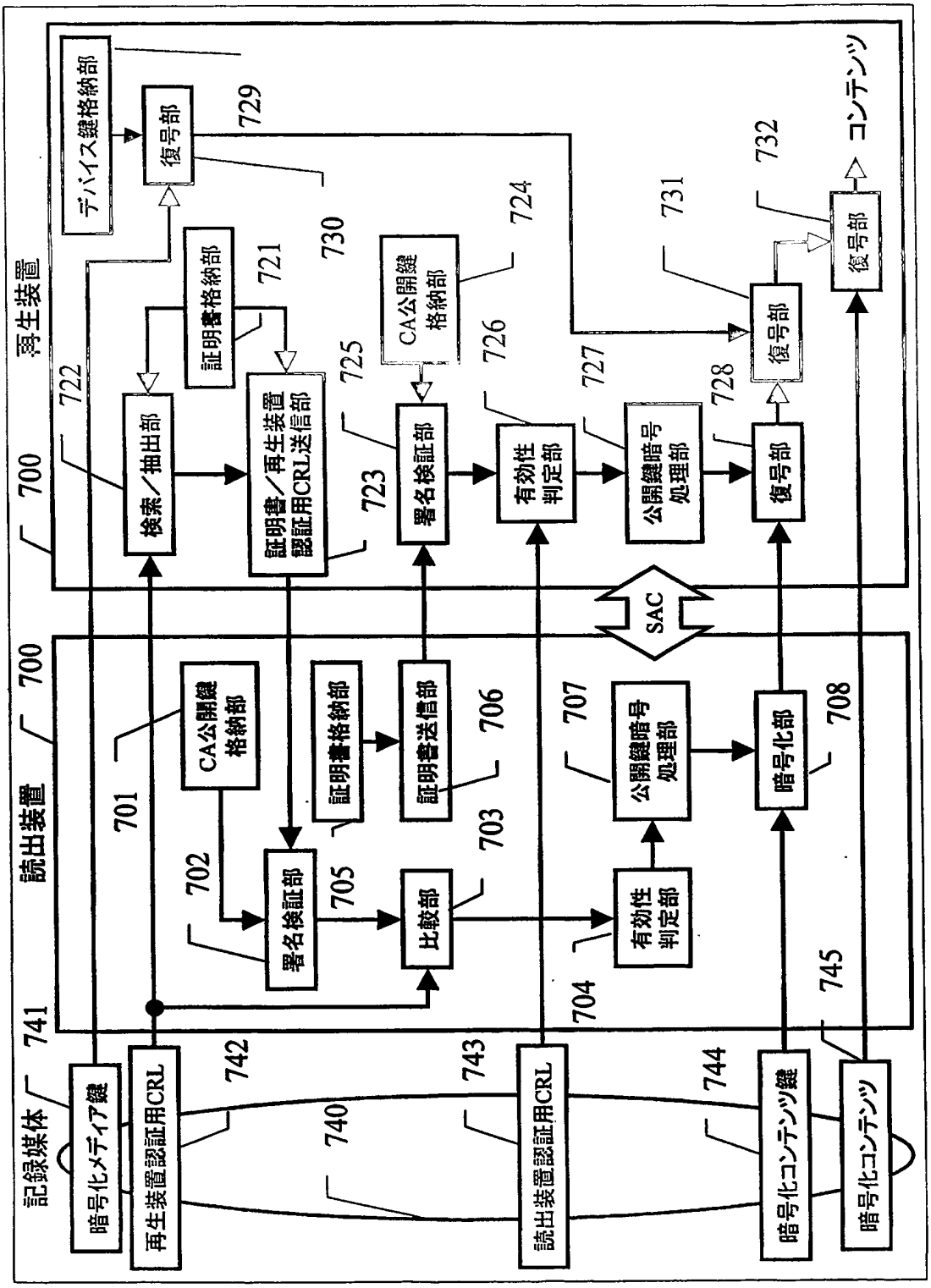
【図５】


再生装置
読出装置
記録媒体
①
S501
受信したCRLのバージョン番号と記録媒体上のバージョン番号が一致するかどうか比較.
S502
一致？
No
Yes
END
S503
証明書が有効かどうか判定.
S504
有効？
No
Yes
END
セッション鍵を生成して，受信した証明書に含まれる公開鍵で暗号化して再生装置へ送信.
S505
受信した暗号化セッション鍵を，保持する秘密鍵で復号してセッション鍵を得る.
S506
②

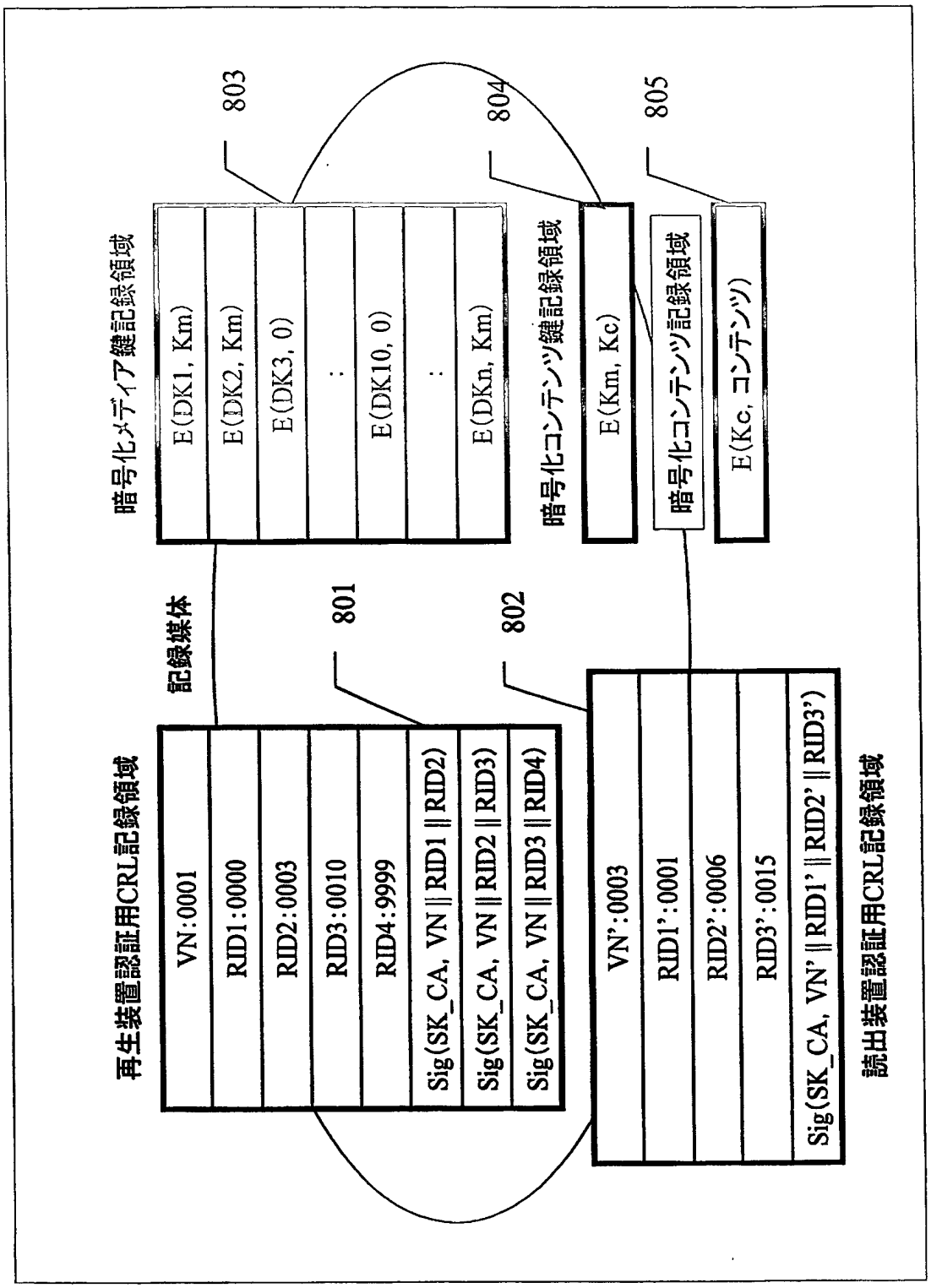
【図６】


記録媒体
読出装置
再生装置
暗号化コンテンツ鍵
暗号化メディア鍵
暗号化コンテンツ
S601
セッション鍵で暗号化コンテンツ鍵を暗号化して再生装置へ送信.
S602
②
受信した2重暗号化されたコンテンツ鍵をセッション鍵で復号して暗号化コンテンツ鍵を得る.
S603
受信した暗号化メディア鍵を，保持するデバイス鍵で復号して，復号して得たメディア鍵で，同じく復号して得た暗号化コンテンツ鍵を復号してコンテンツ鍵を得る.
S604
復号して得たコンテンツ鍵で，暗号化コンテンツを復号してコンテンツを得る.

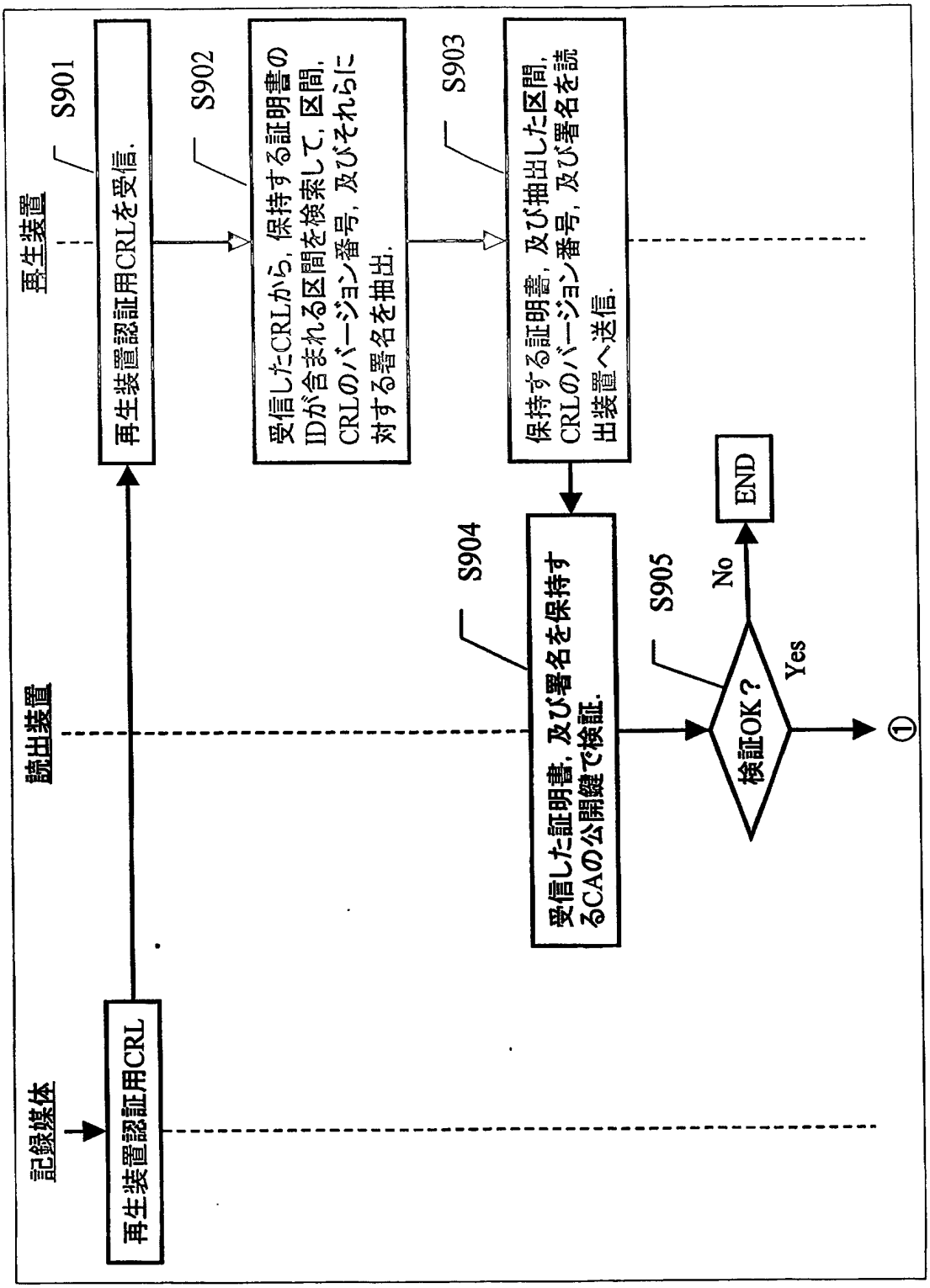
【図７】


記録媒体
読出装置
再生装置
暗号化メディア鍵
再生装置認証用CRL
読出装置認証用CRL
暗号化コンテンツ鍵
暗号化コンテンツ
CA公開鍵格納部
証明書格納部
証明書送信部
署名検証部
比較部
有効性判定部
公開鍵暗号処理部
暗号化部
SAC
デバイス鍵格納部
復号部
検索／抽出部
証明書／再生装置認証用CRL送信部
CA公開鍵格納部
署名検証部
有効性判定部
公開鍵暗号処理部
復号部
復号部
コンテンツ
700
701
702
703
704
705
706
707
708
721
722
723
724
725
726
727
728
729
730
731
732
740
741
742
743
744
745

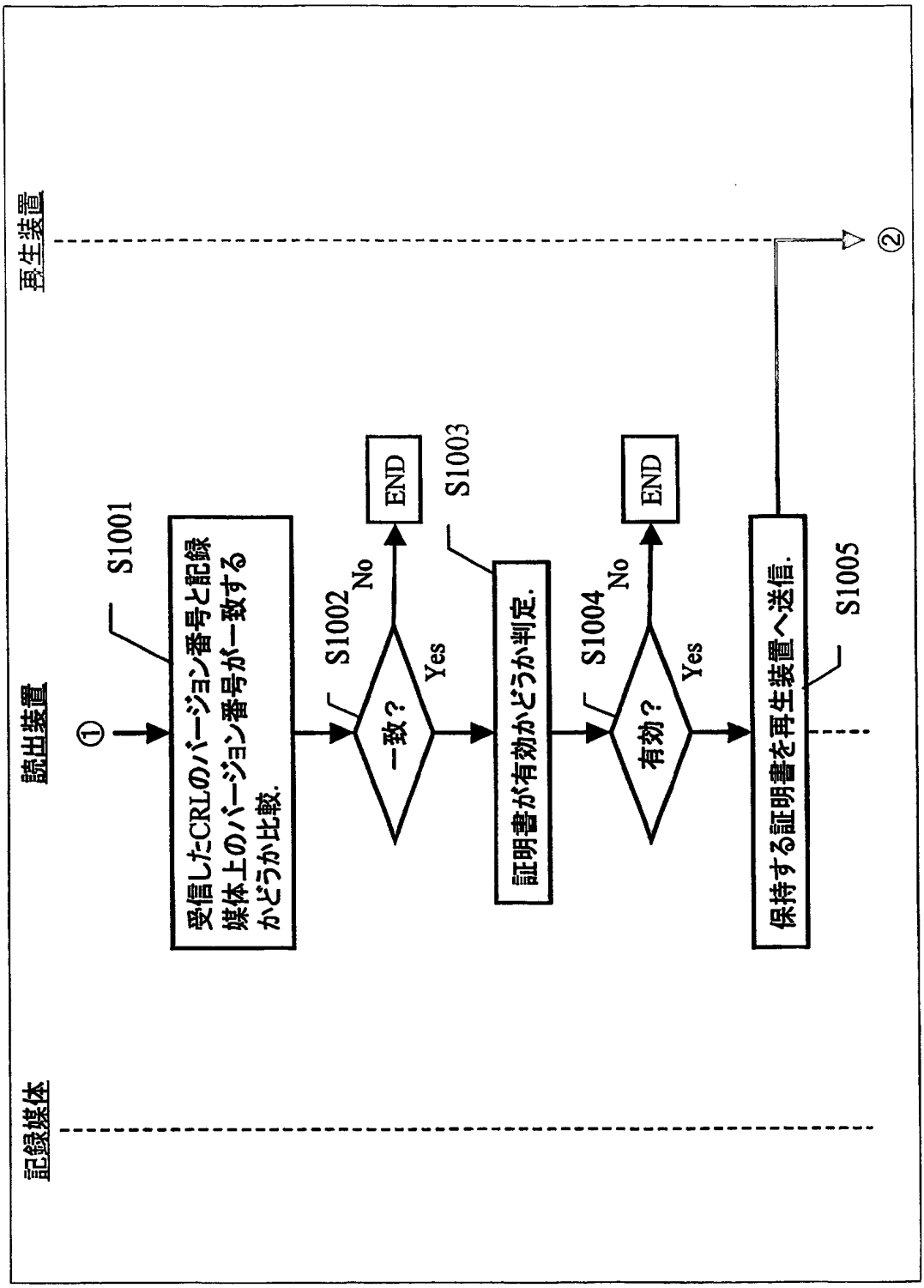
【図８】


再生装置認証用CRL記録領域
VN:0001
RID1:0000
RID2:0003
RID3:0010
RID4:9999
Sig(SK_CA, VN || RID1 || RID2)
Sig(SK_CA, VN || RID2 || RID3)
Sig(SK_CA, VN || RID3 || RID4)
801
記録媒体
802
読出装置認証用CRL記録領域
VN':0003
RID1':0001
RID2':0006
RID3':0015
Sig(SK_CA, VN' || RID1' || RID2' || RID3')
暗号化メディア鍵記録領域
E(DK1, Km)
E(DK2, Km)
E(DK3, 0)
:
E(DK10, 0)
:
E(DKn, Km)
803
804
暗号化コンテンツ鍵記録領域
E(Km, Kc)
805
暗号化コンテンツ記録領域
E(Kc, コンテンツ)

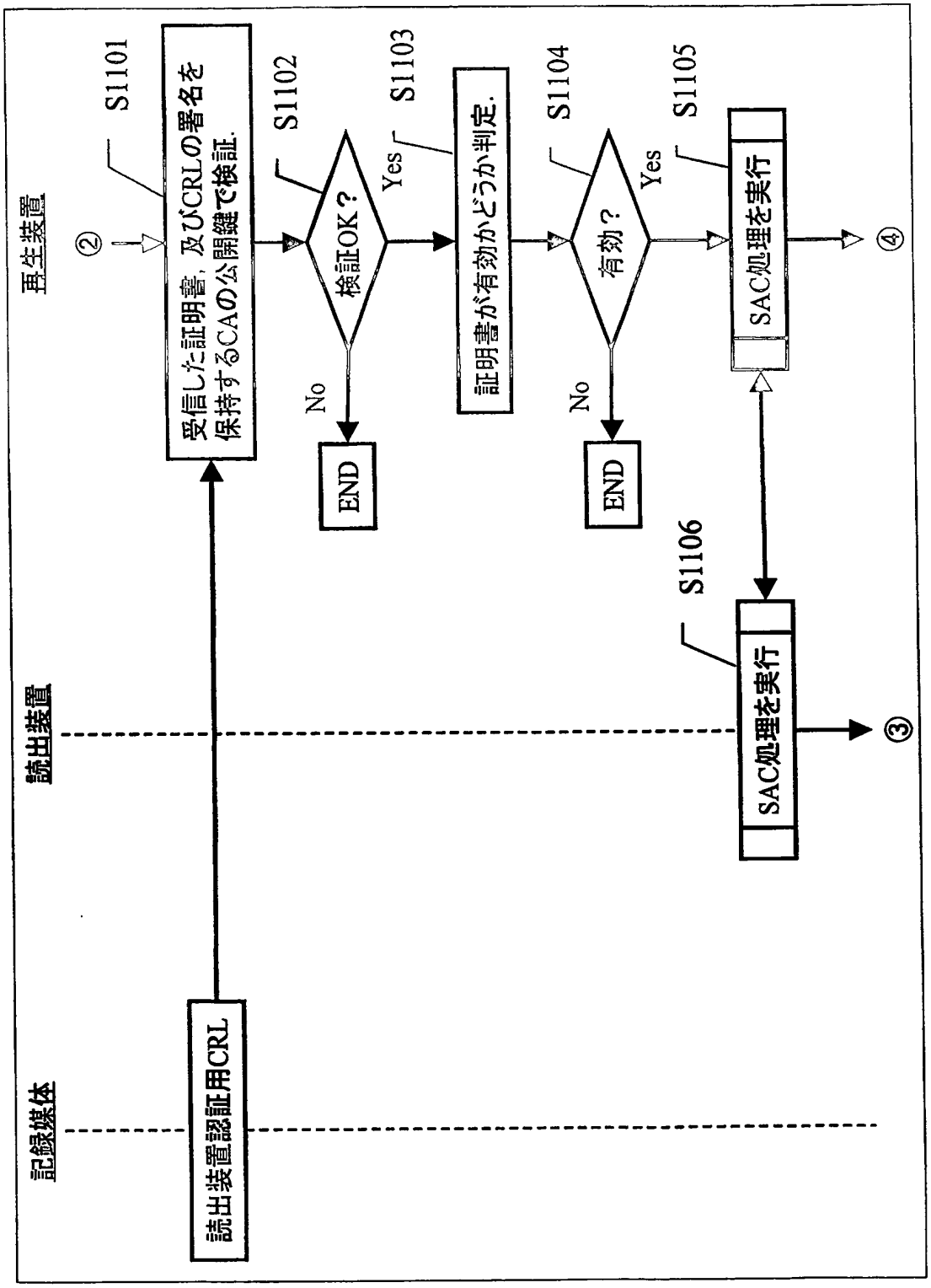
【図９】


記録媒体
再生装置認証用CRL
読出装置
再生装置
再生装置認証用CRLを受信.
S901
受信したCRLから，保持する証明書のIDが含まれる区間を検索して，区間，CRLのバージョン番号，及びそれらに対する署名を抽出.
S902
保持する証明書，及び抽出した区間，CRLのバージョン番号，及び署名を読出装置へ送信.
S903
受信した証明書，及び署名を保持するCAの公開鍵で検証.
S904
検証OK？
S905
No
Yes
END
①

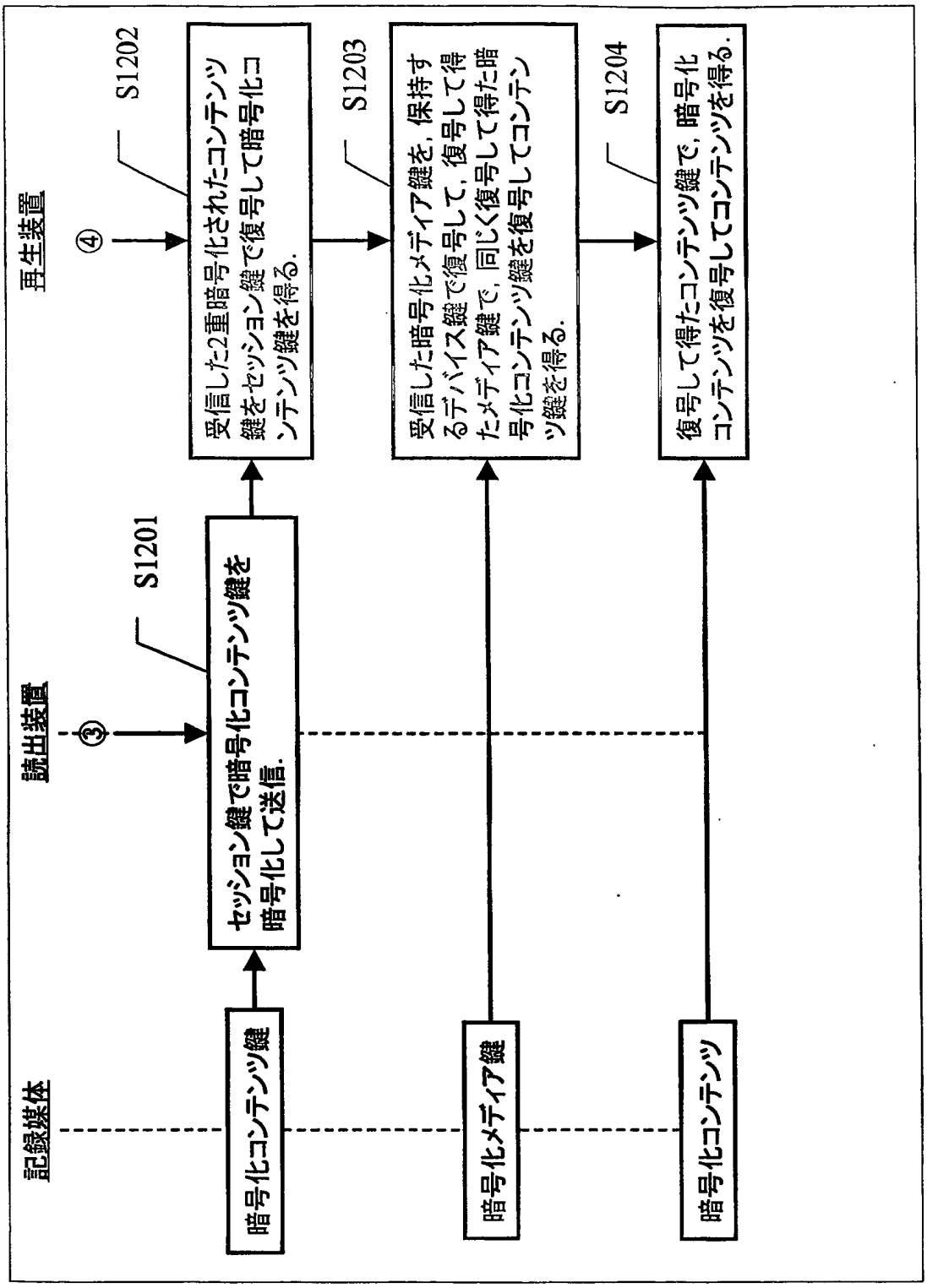
【図１０】


再生装置
読出装置
記録媒体
①
②
S1001
受信したCRLのバージョン番号と記録媒体上のバージョン番号が一致するかどうか比較.
S1002
一致？
No
Yes
END
S1003
証明書が有効かどうか判定.
S1004
有効？
No
Yes
END
S1005
保持する証明書を再生装置へ送信.

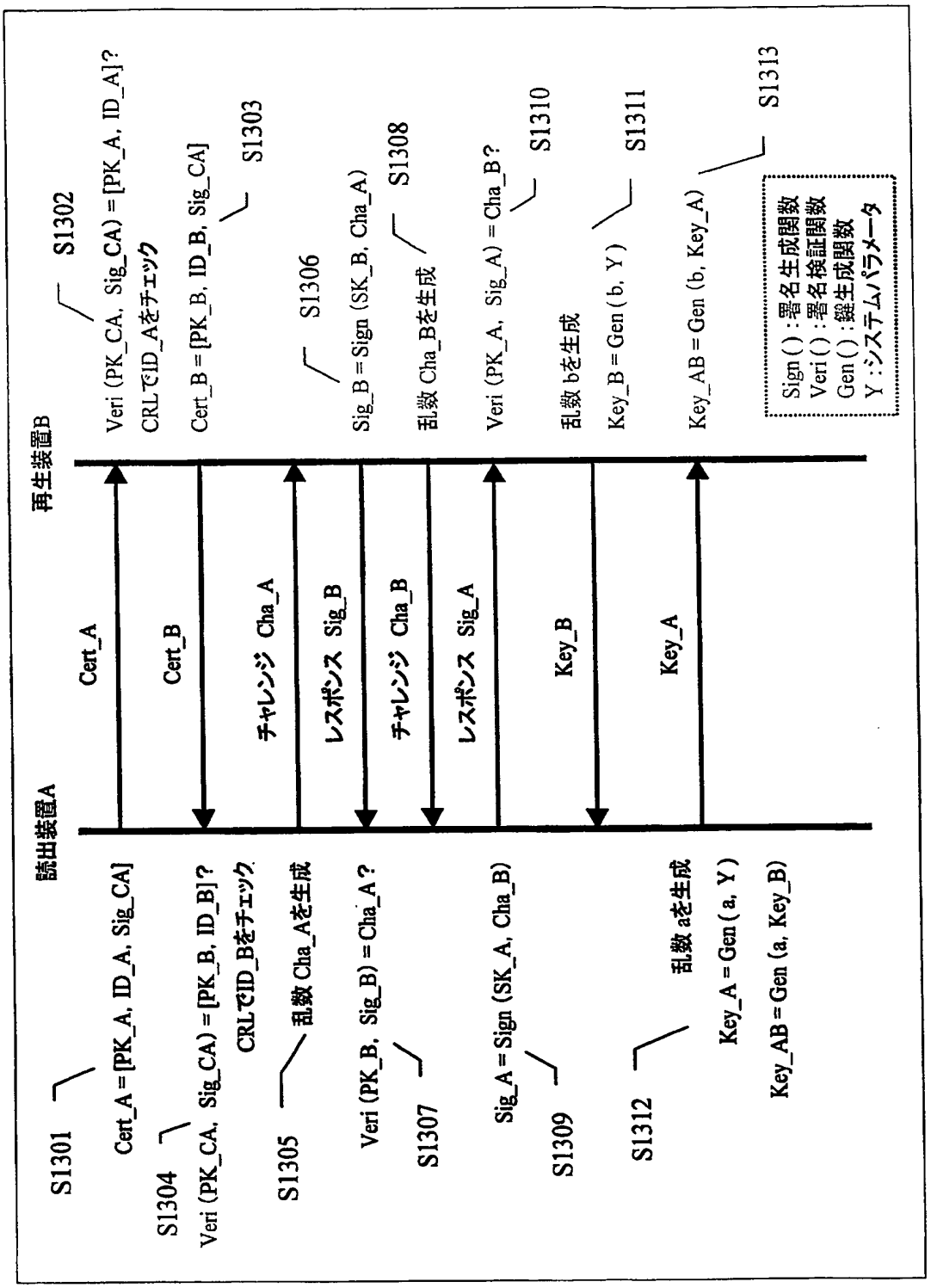
【図１１】


再生装置
読出装置
記録媒体
②
S1101
受信した証明書，及びCRLの署名を保持するCAの公開鍵で検証.
S1102
検証OK？
No
END
Yes
S1103
証明書が有効かどうか判定.
S1104
有効？
No
END
Yes
S1105
SAC処理を実行
④
S1106
SAC処理を実行
③
読出装置認証用CRL

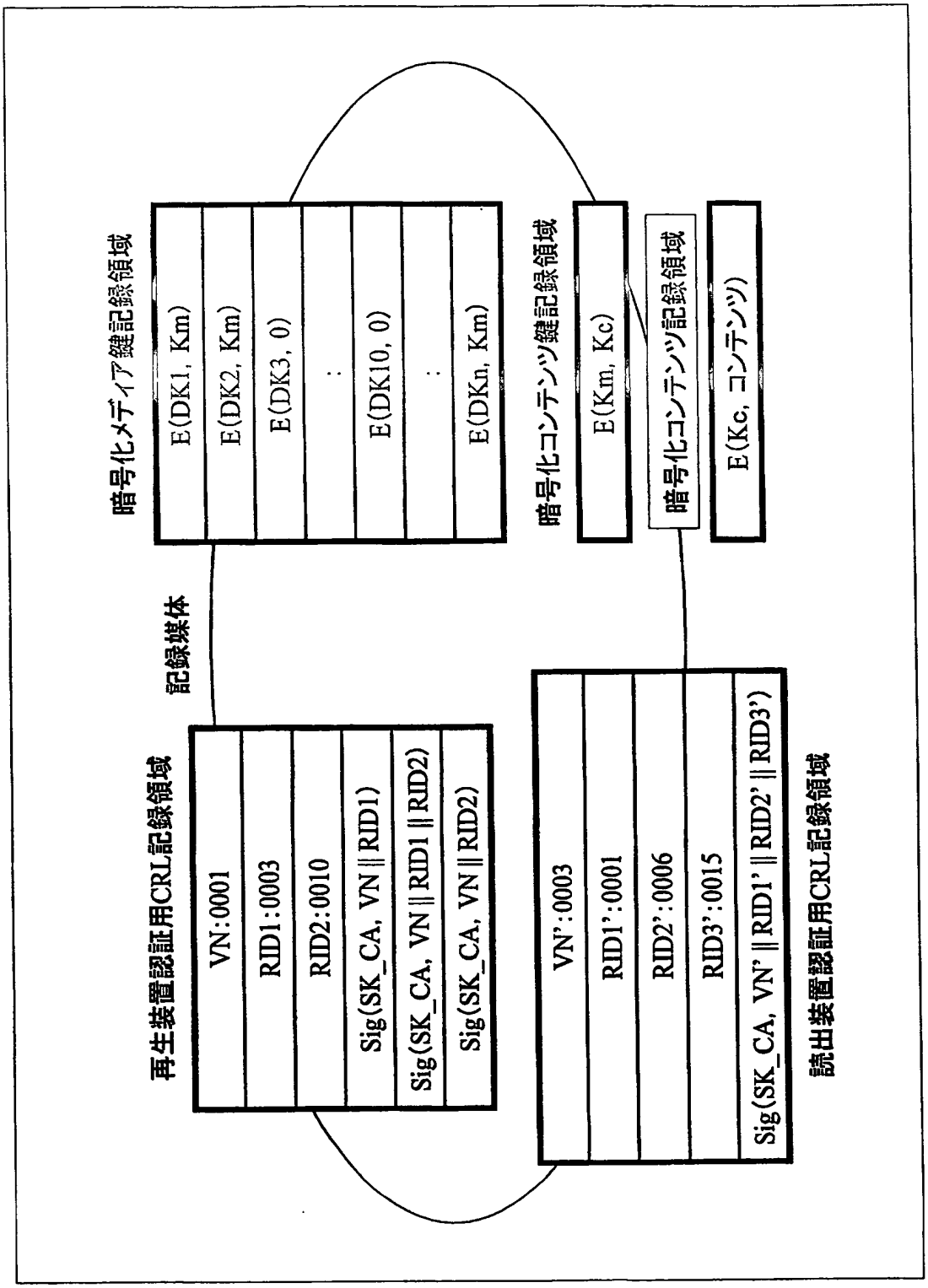
【図１２】


記録媒体
読出装置
再生装置
暗号化コンテンツ鍵
暗号化メディア鍵
暗号化コンテンツ
③
セッション鍵で暗号化コンテンツ鍵を暗号化して送信.
S1201
④
受信した2重暗号化されたコンテンツ鍵をセッション鍵で復号して暗号化コンテンツ鍵を得る.
S1202
受信した暗号化メディア鍵を，保持するデバイス鍵で復号して，復号して得たメディア鍵で，同じく復号して得た暗号化コンテンツ鍵を復号してコンテンツ鍵を得る.
S1203
復号して得たコンテンツ鍵で，暗号化コンテンツを復号してコンテンツを得る.
S1204

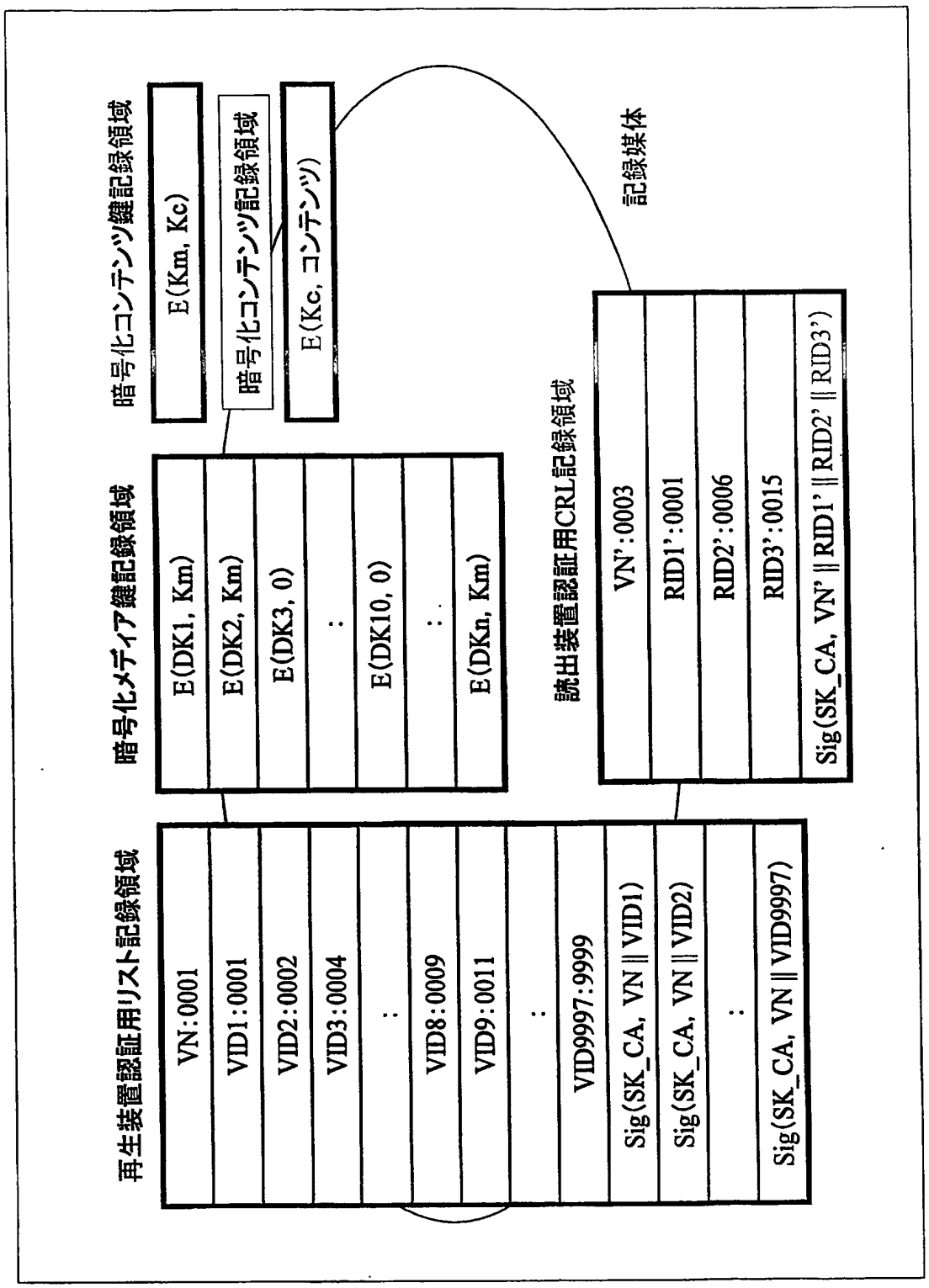
【図１３】


読出装置A
再生装置B
Cert_A
Cert_B
チャレンジ Cha_A
レスポンス Sig_B
チャレンジ Cha_B
レスポンス Sig_A
Key_B
Key_A
S1301
Cert_A = [PK_A, ID_A, Sig_CA]
S1302
Veri (PK_CA, Sig_CA) = [PK_A, ID_A]?
CRLでID_Aをチェック
S1303
Cert_B = [PK_B, ID_B, Sig_CA]
S1304
Veri (PK_CA, Sig_CA) = [PK_B, ID_B]?
CRLでID_Bをチェック
S1305
乱数 Cha_Aを生成
S1306
Sig_B = Sign (SK_B, Cha_A)
S1307
Veri (PK_B, Sig_B) = Cha_A?
S1308
乱数 Cha_Bを生成
S1309
Sig_A = Sign (SK_A, Cha_B)
S1310
Veri (PK_A, Sig_A) = Cha_B?
S1311
乱数 bを生成
Key_B = Gen (b, Y)
S1312
乱数 aを生成
Key_A = Gen (a, Y)
S1313
Key_AB = Gen (a, Key_B)
Key_AB = Gen (b, Key_A)
Sign ( ) : 署名生成関数
Veri ( ) : 署名検証関数
Gen ( ) : 鍵生成関数
Y : システムパラメータ

【図１４】


暗号化メディア鍵記録領域
E(DK1, Km)
E(DK2, Km)
E(DK3, 0)
:
E(DK10, 0)
:
E(DKn, Km)
暗号化コンテンツ鍵記録領域
E(Km, Kc)
暗号化コンテンツ記録領域
E(Kc, コンテンツ)
記録媒体
再生装置認証用CRL記録領域
VN:0001
RID1:0003
RID2:0010
Sig(SK_CA, VN || RID1)
Sig(SK_CA, VN || RID1 || RID2)
Sig(SK_CA, VN || RID2)
VN':0003
RID1':0001
RID2':0006
RID3':0015
Sig(SK_CA, VN' || RID1' || RID2' || RID3')
読出装置認証用CRL記録領域

【図１５】


再生装置認証用リスト記録領域
VN:0001
VID1:0001
VID2:0002
VID3:0004
VID8:0009
VID9:0011
VID9997:9999
Sig(SK_CA, VN || VID1)
Sig(SK_CA, VN || VID2)
Sig(SK_CA, VN || VID9997)
暗号化メディア鍵記録領域
E(DK1, Km)
E(DK2, Km)
E(DK3, 0)
E(DK10, 0)
E(DKn, Km)
暗号化コンテンツ鍵記録領域
E(Km, Kc)
暗号化コンテンツ記録領域
E(Kc, コンテンツ)
読出装置認証用CRL記録領域
VN':0003
RID1':0001
RID2':0006
RID3':0015
Sig(SK_CA, VN' || RID1' || RID2' || RID3')
記録媒体

【書類名】要約書
【要約】
【課題】　公開鍵暗号を利用した認証システムにおいて、ＣＲＬのサイズが大きくなった場合であってもドライブの処理負荷を軽減する。
【解決手段】　ドライブがホストを認証する場合であっても、ホストがＣＲＬを検索してドライブに結果を送信し、その検索結果を受信したドライブが、検索結果の正当性を検証するのみでホストの認証を実現することにより、認証システムにおけるドライブの処理負荷を軽減する。
【選択図】　図１

特願２００３－２７１９２９

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社